Response to Pre-Bid Queries Received
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

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
Firm Name:- **Recorded Future**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**
1	4.1 Pre-Qualification(PQ)/ Eligibility Criteria , 4. OEM Experience	20	Documents Required : Customer PO copies, completion certificate and any feedback from the client.	Generally PO are covered under NDA as it's related to cyber security, so pls add reference call with the customer for PQ qualification. May be changed as , " Documents Required : Customer PO copies OR completion certificate OR any reference call for feedback from the existing client. The customer contact details need to be shared as a part of PQ"	Clause Amended:- Please refer corrigendum
2	4.1 Pre-Qualification(PQ)/ Eligibility Criteria 5. Technical Capability	21	Package – II "Similar Nature" is defined as: supply, installation & support of Enterprise Security Solution (Threat Intel Platform & Web Scanning Tool should be the major component and should be inclusive of all three solutions) Government/Semi Government/ PSU/ Scheduled Banks.	Under Package II Threat Intel Platform & Web Scanning tool are generally from different OEMs. We request you to consider the POs for these items separately for the asked value.	The Bidder/OEM may submit Separate PO copies for Threat Intel Platform & Web Scanning Tool, but the PO should be

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					issued from same customer within the last three financial year i.e. 2020-21, 2021-22 & 2022-23. Also aggregate value of POs should be as per Project values asked in Technical Capabilities Section.
3	4.1 Pre-Qualification(PQ)/ Eligibility Criteria 6. Quality Certifications	22	Bidder and OEM should have ISO 9001:2015, ISO 20000:2018, ISO 27001:2013 / ISO 27001:2022 Certifications.	The PQ ask is not in line with the technical requirement. may please be changed as : "Bidder/OEM should have ISO 9001:2015, ~~ISO 20000:2018~~, ISO 27001:2013 / ISO 27001:2022 and ISO/IEC 27701:2019 Certifications.	Clause Amended:- Please refer corrigendum
4	21.2.2 Package II 7. Quality Certifcations	50	Quality Certifications : ISO 9001:2015, ISO 20000:2018 ISO 27001:2013 / ISO 27001:2022	The PQ ask is not in line with the technical requirement. may please be changed as : "ISO 9001:2015, ~~ISO 20000:2018~~, ISO 27001:2013 / ISO 27001:2022 and ISO/IEC 27701:2019 Certifications.	Clause Amended:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
5	21.5.2.1. Specification for Threat Intel Solution, Platform	59	Vendors' staff assigned to the project must hold professional certifications related to cybersecurity such as: GNFA, GCIH, CISM, CISA, CISSP.(Preferred)	Please add CEH to the asked requirement .May change as "Vendors' staff assigned to the project must hold any of the following professional certifications related to cybersecurity such as: GNFA, GCIH, CISM, CISA, CEH, CISSP"	As per RFP
6	21.5.2.1. Specification for Threat Intel Solution, Threat Intelligence Feed Requirement	61	• Registration organization – Name of the registration organization. • Registrar name – Name of the domain name registrar. • Owner name – Domain owner name. • Category – Category of the requested URL. • Owner name – Name of the requested IP address owner. • Owner ID – ID of the requested IP address owner.	Generally this information is subject to availability as post GDPR implementation RABT details on domains are generally masked/Redacted hence the asked field information may only be partially available for IP and Domains. It is requested that the asked fields may be dropped from the RFP.	It is the requirement. However, owing to legal complicacy partially available information is acceptable. But during verification of Partial Details of information OEM should provide proper justification.
7	21.5.2.1. Specification for Threat Intel Solution	62	Platform should provide OT/ICS Threat Intel feeds with interactive dashboard.	May be changed as " Platform should provide OT/ICS Threat Intel feeds/IOCs with interactive dashboard showing top Threat Actors/Ransomwares impacting an industry or industry peers"	It's the minimum requirement of the solution. The OEM can provide more information to

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					enrich the environment.
8	21.5.2.1. Specification for Threat Intel Solution, Darkweb and Deepweb Monitoring	65	The platform should incorporate a range of multi- layered monitoring services and analysis techniques and correlates data across a range of resources including: - .onion sites, I2P sites and alternative networks; - Dark Net blogs, forums, chat rooms; - Infostealer Marketplaces, Logs and Cookies - IRC conversations; - Black market and criminal auction sites - Ransomware forums - Telegram	IRC has been replaced with Discord channels and generally not a useful source for Threat Intelligence. This may be changed as below : IRC conversations/Discord	Clause Amended:- Please refer Corrigendum
9	21.5.2.1. Specification for Threat Intel Solution, Brand Inte.ligence	67	The platform should monitor all the major social media platform, including, but not limited to; Twitter, Facebook, YouTube, Instagram, LinkedIn, Tiktok,Vimeo, RSS All data sources should be collectively analyzed for the use of Customer's brand. These should be reviewed by bidder's /	Meta platform limits automated data collection from its platform like Facebook, Instagram, hence may please be removed. Please refer Facebook policy at https://www.facebook.com/apps/site_scraping_tos_terms.php Also video platforms like TikTok and Vimeo may also be removed for similar reasons.	Clause Amended:- Please refer Corrigendum
10	21.5.2.1. Specification for Threat Intel Solution, Brand Monitoring	67	Platform should be capable of doing Image/Logo monitoring to identify profile impersonation	Image and Logo Monitoring are 2 different technologies which may be used together or seperately to moniter various Brand impersonation cases. Hence may be changed as	Clause Amended:- Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
				" Platform should be capable of doing both Image OCR and Logo monitoring to identify profile or company impersonation"	
11	21.5.2.1. Specification for Threat Intel Solution	68	OEM Should have their own in-house takedown mechanism and not rely on 3rd- party services.	This clause limits our participation to the RFP. Many OEM solutions have tie ups with third parties for take down services. It is requested to change the clause to "OEM Should have a takedown mechanism natively in their solution either directly or via native platform integration with any 3rd-party services."	Clause Amended:- Please refer Corrigendum
12	21.5.2.1. Specification for Threat Intel Solution, support	74	Incident Response Services (a) On-demand Malware Analysis and Reverse Engineering Assistance (b) On-demand Computer Forensics Analysis, Log Analysis, and Investigation	Please mention the number of on-demand Analyst services required in the scope of RFP	Clause Deleted Please refer Corrigendum
13	21.5.2.1. Specification for Threat Intel Solution, Intelligence on Leaked Credentials	71		Please clarify the number of employees of OCAC and domains for which credential leaks monitoring is required	Bidder/OEM may understand the client infrastructure/ user strength to get the information and propose the solution at it's own

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
14	21.5.2.1. Specification for Threat Intel Solution,	59		Please clarify the number of analysts of OCAC which shall be working on the Threat Intel Solution	Bidder/OEM may understand and suggest for the ideal proposition
Firm Name:- **Infinity Labs**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**
1	21.5.2.2 Specification for Threat Integration Platform	80	Request for Addition of New Clause: Workflow-based Automation: 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.	To automate generation of IOCs lists for different products some level of automation is recommended within the Threat Integration Platform	Accepted Please refer corrigendum
Firm Name:- **Fortinet**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**
1	1.8		The appliance should have minimum internal storage of 400 GB SSD for Logs & Reports or better.	The appliance should have minimum internal storage of 1TB SSD for Logs & Reports or better. OEM specific point, for longer period of storing logs we suggest to have separate Syslog server.	It's already mentioned the RFP about that "The appliance should have minimum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					internal storage of 1TB SSD for Logs & Reports or better."
2	3.4		The appliance should have minimum Antivirus Throughput of 12 Gbps or better	Remove this point This ia OEM specific point, not published by all Firewall OEM. Request you to amend the clause as " The appliance should have minimum 10 Gbps of Threat Prevention Throughput measured with Firewall, IPS, Application Control, and Malware Protection enabled, Enterprise Mix traffic" this point to make this generic so that all leaders OEM can participate.	Please refer corrigendum
3	3.6		The appliance should have minimum Firewall IMIX Throughput of 28 Gbps or better	Remove this point This is not standard parametrs published by all OEMs.	IMIX throughput consideration of Real World/Prod Performance Under Test Condition in Gbps. The IMIX throughput in Data Centre firewall require to handle a large

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					volume of diverse traffic, including network/server access of datacentre. This is in generic requirement/parameter which is available with most of firewall OEM's.
4	3.8		The appliance should have minimum 40000 Number of IPSec VPN Peers supported (Site to Site)	The appliance should have 2000 numbers of IPSEC VPN Peers supported (Site to Site) OEM specific point and 40,000 Site to Site VPN support with only 13 Gbps of VPN throughput asked in the point no. 3.7 is not matching.	Please refer corrigendum
5	3.11		The appliance should have minimum 20M Concurrent Session/Concurrent Connection	The appliance should have minimum 5 million Concurrent Session/Concurrent Connection 20 Million concurrent session/ concurrent connections is too high considering only 500K new sessions per second and considering others performance parameters. Hence we request you to amend the clauses as "The appliance should have minimum	Any traffic session hitting the Data Centre network/server is unpredictable, So higher Concurrent sessions

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
				5 million Concurrent Session/Concurrent Connection"	required to scale and accommodate the growing number of devices and users accessing the network in Data Centre. Higher concurrent session/concurrent connection require to process high volume of traffic in the event of DOS/DDOS attacks, security events, and anomalies, which cause surge of concurrent sessions and prevent / hamper connection of

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					data centre Hence, there is a requirement of high concurrent connections in data Centre firewall.
6	3.14		The appliance Should support 25000+ IPS Signature for future upgradation of Next generation IPS license	The appliance should have support 10,000 + IPS signature and support for custom IPS signature creation. Not all OEMs support the asked parameters, request you to amend the clause as "The appliance should have support 10,000 + IPS signature and support for custom IPS signature creation." to ensure maximum particiaption.	Higher number of IPS signatures increase the breadth of threat coverage and actively blocking potentially malicious traffic based on signatures. Since asked 25000+ signatures are available with majority of the OEM and there is no requirement

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					of custom IPS signatures. Since OEM tested IPS signatures are more reliable and secure than custom signatures.
7			The proposed OEM should Comply with Make in India as per Public Procurement Act (Preference to Make in India)	Remove this point Request you to change this point, so that all Leaders OEM can participate	Accepted Please refer corrigendum
8			The product shall comply minimum 60% and Above Local content or higher	Remove this point Request you to change this point, so that all Leaders OEM can participate.	Accepted Please refer corrigendum
Firm Name:- **Cyble**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**
1	4.1 , Pt 6	22	Bidder and OEM should have ISO 9001:2015, ISO 20000:2018, ISO 27001:2013 / ISO 27001:2022 Certifications	Cyble has ISO 27001 and SOC2 certificate which covers all of necessary compliances required in other certificates. For this solution, Request for modification "**bidder and OEM should have ISO 27001 and SOC2 certification**" as this will keep certifications simple and will still include all required compliances	Clause Amended:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
2	21.5.2.1	59	The OEM solution must comply to the following certifications: A. ISO/IEC 27701:2019 for Privacy Information Management System B. ISO 9001 Compliant	Cyble has ISO 27001 and SOC2 certificate which covers all of necessary compliances required in other certificates. For this solution, Request for modification "**bidder and OEM should have ISO 27001 and SOC2 certification**" as this will keep certifications simple and will still include all required compliances	Clause Amended:- Please refer corrigendum
3	21.5.2.1	62	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	Request you to keep SLA per day for the IOCs as IOCs are updated based on dynamic ratings, and it automatically starts deprecting the score with time. This keeps the score similar whether the scan is done every hour or every day.	As per RFP
4	21.5.2.1	66	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. For image results there should be an option to disable viewing/blurring of images or reporting it.	Will this be required as feed or as cases in the RFP? While we will include the images from the platforms, Cyble doesn't get slow from any image processing, so we can display the images without having any lag.Disabling and Blurring of images is a feature very specific to one OEM, **so we request you to kindly remove it.**	Clause Amended:- Please refer corrigendum
5	21.5.2.1	71	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	Apart from credentials, these malware also steal a lot of files from the infected endpoint. **We request you to also add that files being taken out of the system should also be monitored for OCAC data**	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
6	21.5.2.1	71	The solution must have option to restrict view of cleartext password for limited admin users only	Restriction in Cyble can be done on the feature itself. Basically, a user can be restricted in accessing the feature or feature upto a certain limit. This allows people without admin acess in a restricted manner. Please suggest if this will be okay for the RFP.	Yes, Bidder's understating is correct
7	21.5.2.1	72	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.	**This can be done without a plugin.** Will that suffice the requirement. Plugin is limited for one OEM only, and we therefore we request yout o make it conditional.	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome.

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
8	21.5.2.1	72	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 IOCs being shown on the page for reducing triage time for analyst.	T**his can be done without a plugin**. Will that suffice the requirement. Plugin is limited for one OEM only, and we therefore we request yout o make it conditional.	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
9	21.5.2.1	72	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, Domain, 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 extension 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.	These points are limited to one OEM only. These ate private specs for the same, and we request you to remove them as will it be favorable only that OEM.	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
10	21.5.2.1	73	The browser extension must have the capability to upload suspicious file URLs for detonation and analysis to OEM offered sandbox solution	This can be done without a plugin. Will that suffice the requirement. Plugin is limited for one OEM only, and we therefore we request yout o make it conditional.	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
11	Additional Point to add in the specification	Additional Point	We also suggest that AD integration will be present for the solution, so that OCAC can clearly differentiate between data of current users of OCAC vs old users of OCAC	Additional Point to add in the specification	Bidder have to provide the solution based on present environment.
Firm Name:- **Cloudsek**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**
1	21.5.2.1. Specification for Threat Intel Solution	59	Vendor must have Minimum 10 years expertise in anti–malware research/Threat Research	We would request you to consider minimum 7+ years expertise in antimalware research/Threat research	Clause Amended:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
2		59	Platform should provide the UI in multiple languages(Eg.(i) Arabic (ii) Chinese (both simplified and traditional script) (iv) Farsi (Persian) (v) French (vi) German (vii) Japanese (viii) Russian (ix) Spanish (x)English) & support Summarization & translation of the information	Platform supports scraping the data from multiple languages and from sources across the globe, but the UI itself doesn't have that capability	Clause Amended:- Please refer corrigendum
3		59	The OEM solution must comply to the following certifications:A. ISO/IEC 27701:2019 for Privacy Information Management System B. ISO 9001 Compliant	We would request you to consider ISO 27001 and ISO 9001	Clause Amended:- Please refer corrigendum
4		60	Platform should provide an IOC Lookup feature, where customer will get IOC Risk Score, Confidence Score, Source details, TA profile & IOA	CloudSEK platform currently doesn't have a UI based IOC lookup feature, although IOCs are being provided to the clients	As per RFP
5		62	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	This would be a part of the IOC lookup feature not being currently covered	As per RFP
6		66	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.	This would be a part of the IOC Lookup feature not being covered	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
7		67	Social Media Monitoring: The platform should monitor all the major social media platform, including, but not limited to; Twitter, Facebook, YouTube, Instagram, LinkedIn, Tiktok,Vimeo, RSS All data sources should be collectively analyzed 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. 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	CloudSEK platform has a rich source inventory where multiple sources for brand related issues including but not limited to social media platforms like Facebook, Twitter, Instagram, LinkedIn, and video sharing websites like YouTube are indexed. Any mentions of the client assets across these sources would be detected and contexualised on the platform. These mentions are then also manually analysed and verified by a team of security researchers and proactive alerts are sent to the client to mitigate these threats TikTok and Vimeo are not being covered as sources yet	Clause Amended:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
8		67	The Bidder/OEM should be member of International Anti-Phishing Working Group (APWG). Solution should provide the visibility of DNS records, Whois records, MX records, screenshot tagged to a typoquatted domain Solution should provide Domain Watclisting feature, to get instant alert whenever there's a change in the status of domain Platform should be capable of doing Image/Logo monitoring to identify profile impersonation Finding domains and emails mentions on Code Repository websites like Github etc CXOs fake social media profiles, posts, pages and groups, takedown is also expected here.	CloudSEK complies with all the requirements ,however Cloudsek isnt a member of APWG. We request you to kindly consider this.	Clause Amended:- Please refer corrigendum
9		70	The solution should show information about spam attacks in which the requested object is attached to email messages.	Feature not being covered, Requesting you to kindly remove the point as it is OEM specific	Clause Deleted Please refer Corrigendum
10		71	The solution must have option to restrict view of cleartext password for limited admin users only	Since CloudSEK already has a feature to create role-based access controls where the accesses themselves can be modularised, we kindly request you to remove this point from the specifications	As per RFP. If the Role Based access control suffice the requirement of RFP then it is acceptable

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
11		71	Clicking links in documents for Microsoft Office (Word, Excel, PowerPoint, Publisher, Outlook) and Adobe Reader	CloudSEK would be able to detect any documents containing mentions of the client's assets, although the links present in those documents would not be scanned for. Requesting to kindly consider this iterations	Clause Amended:- Please refer corrigendum
12		72	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.	Browser extension not being offered, Requesting you to kindly remove the point as it is OEM specific	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
13			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 critical, medium and low severity.		The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
14			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 IOCs being shown on the page for reducing triage time for analyst		The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
15			The browser extension must have capability to block potentially malicious links on the webpage being reviewed by the analyst		The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					desired outcome
16			The browser extension must have the option to enable or disable automatic detection of IOCs like IP, Domain, URL, hash and vulnerability (CVE)		The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
17			The browser extension must work with the following solutions Anomaly ThreatStream, ArcSight ESM, ELK (Dashboard only), MISP, Qualys, The Hive Project, VirusTotal etc		The OEM needs to justify and demonstrate how they can perform the IOC

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
18			The browser extension 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 OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					plugin or any similar way to achieve the desired outcome
19			The browser extension must have the capability to upload suspicious file URLs for detonation and analysis to OEM offered sandbox solution.		The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
20		73	Dynamic Malware Sandboxing should be available: The service should support malware sandboxing by allowing users to a. Upload suspicious files to the platform and download a detailed file behavior analysis report and network analysis report for each uploaded file 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 c. The sandbox should protect organizational privacy by not uploading the file to any publicly accessible repository or third party B. The sandboxing should support operating systems such as Windows, Linux, Mac IoS & Android at a minimum. C. The service should support automated analysis of at-least 50 samples per dayD. The service provider should provide analyst support for report interpretation and explanation as and when required.	Sandbox not being offered, Requesting you to kindly remove the point as it is OEM specific	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
21		73	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	MITRE ATT&CK Framework is being followed for report creation	As per RFP
22		73	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		As per RFP
23		74	Incident Response Services (a) On-demand Malware Analysis and Reverse Engineering Assistance (b) On-demand Computer Forensics Analysis, Log Analysis, and Investigation	CloudSEK currently does not provide incident response services, Requesting you to kindly remove the point as it is OEM specific	Clause Deleted Please refer Corrigendum
Firm Name:- **HPE**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**
1	4.1 , Pt 6	22	Bidder and OEM should have ISO 9001:2015, ISO 20000:2018, ISO 27001:2013 / ISO 27001:2022 Certifications	Cyble has ISO 27001 and SOC2 certificate which covers all of necessary compliances required in other certificates. For this solution, Request for modification "**bidder and OEM should have ISO 27001 and SOC2 certification**" as this will keep	Clause Amended:- Please refer corrigendum.

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
				certifications simple and will still include all required compliances	
2	21.5.2.1	59	The OEM solution must comply to the following certifications: A. ISO/IEC 27701:2019 for Privacy Information Management System B. ISO 9001 Compliant	Cyble has ISO 27001 and SOC2 certificate which covers all of necessary compliances required in other certificates. For this solution, Request for modification "**bidder and OEM should have ISO 27001 and SOC2 certification**" as this will keep certifications simple and will still include all required compliances	Clause Amended:- Please refer corrigendum
3	21.5.2.1	62	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	Request you to keep SLA per day for the IOCs as IOCs are updated based on dynamic ratings, and it automatically starts deprecting the score with time. This keeps the score similar whether the scan is done every hour or every day.	As per RFP
4	21.5.2.1	66	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. For image results there should be an option to disable viewing/blurring of images or reporting it.	Will this be required as feed or as cases in the RFP? While we will include the images from the platforms, Cyble doesn't get slow from any image processing, so we can display the images without having any lag.Disabling and Blurring of images is a feature very specific to one OEM, **so we request you to kindly remove it.**	Clause Amended:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
5	21.5.2.1	71	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	Apart from credentials, these malware also steal a lot of files from the infected endpoint. **We request you to also add that files being taken out of the system should also be monitored for OCAC data**	As per RFP
6	21.5.2.1	71	The solution must have option to restrict view of cleartext password for limited admin users only	Restriction in Cyble can be done on the feature itself. Basically, a user can be restricted in accessing the feature or feature upto a certain limit. This allows people without admin acess in a restricted manner. Please suggest if this will be okay for the RFP.	Yes, Bidder's understating is correct
7	21.5.2.1	72	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.	**This can be done without a plugin.** Will that suffice the requirement. Plugin is limited for one OEM only, and we therefore we request yout o make it conditional.	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					similar way to achieve the desired outcome
8	21.5.2.1	72	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 IOCs being shown on the page for reducing triage time for analyst.	T**his can be done without a plugin**. Will that suffice the requirement. Plugin is limited for one OEM only, and we therefore we request yout o make it conditional.	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
9	21.5.2.1	72	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, Domain, 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 extension 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.	These points are limited to one OEM only. These ate private specs for the same, and we request you to remove them as will it be favorable only that OEM.	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
10	21.5.2.1	73	The browser extension must have the capability to upload suspicious file URLs for detonation and analysis to OEM offered sandbox solution	This can be done without a plugin. Will that suffice the requirement. Plugin is limited for one OEM only, and we therefore we request yout o make it conditional.	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
11	Additional Point to add in the specification	Additional Point	We also suggest that AD integration will be present for the solution, so that OCAC can clearly differentiate between data of current users of OCAC vs old users of OCAC	Additional Point to add in the specification	Bidder have to provide the solution based on present environment.
12	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should support (DAST) dynamic application security testing. The proposed solution should provide as SaaS offering that is hosted from within India location data centers.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause asks for Saas offering, hence request to please change this point as below The proposed solution should support (DAST) dynamic application security testing. The proposed solution should be deployed on premise with unified/single console for existing Infra Vulnerability management & Web application scanning solution part of this RFP.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
13	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose elastic asset licensing.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum
14	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution must allow users to scan their RESTful API endpoints by providing a Swagger or OpenAPI specification file.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
15	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose unified Web App Scanning and Vulnerability Management.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should propose unified console for Web App Scanning procured under this RFP and existing Infra Vulnerability Management Solution.	Please refer corrigendum
16	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should be hosted on the cloud.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should be deplyed on premise.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
17	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should achieve SSAE16 SOC 2 and/or CSA Star certification.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum
18	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose cloud and on-prem scanners.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should offers on premise scanners.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
19	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose scanners that managed by the platform, e.g. updates to vulnerability signatures, code, and other updates.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below 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.	Please refer corrigendum
20	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt data at rest - data is stored on encrypted media using at least one level of AES-256 encryption.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
21	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt data in transit - data is encrypted in transport using TLS v1.2 with a 4096-bit key (this includes internal transports)	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum
22	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt sensor communication – Traffic from the sensors to the platform is always initiated by the sensor and is outbound-only over port 443. Traffic is encrypted via SSL communication using TLS 1.2 with a 4096-bit key.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
23	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support Single sign-on (SSO) authentication methods.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum
24	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support Two-Factor Authentication (2FA).	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
25	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should have disaster recovery procedures and redundancies in place to minimize disruption.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum
26	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should service strive to provide a 99.95% or better uptime.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
27	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should be able to partition/segregate customer data from other users.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum
28	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should not access, store, or process any Personally Identifiable Information (PII) or Protected Health Information (PHI).	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
29	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should have all data in all states in the cloud platform is encrypted with at least one level of encryption, using no less than AES-256.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum
30	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should propose unified modern attack surface visibility.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
31	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support the ability to produce reports in the following report formats: Json, CSV, XML.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should support the ability to produce reports in the following report formats: CSV & PDF.	Please refer corrigendum
32	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	License to be Provided No .of FQDNs- Minimum 1000 FQDNs	Sizing Queries:- 1. Please provide the Number of location hosting these applications. 2. Data retention policy for Web application scanning data.	1. Please provide the Number of locations hosting these applications- On-Premise Solution. Console to be deployed at Central Location and Scanner to be placed as multiple locations as per OCAC's critical infrastructure.

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					2. Data retention policy for Web application scanning data.- 180 Days
33	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 :- Section :- 21.5.2.4. Project Citation Format	85	Project Citation Format	We request to please confirm if project citation can be provided for Saas/on premise deployment for WAS solution, as funtionality of the solution is similar only model of deployment is as per client requirement.	Project Citation can be provided for SaaS/on premise deployment of WAS Solution
34	1. Fact Sheet	9	Proposals must remain valid till 180 days after the last date of submission of the bids.	Bidder request to reduce the bid validity to 90 days	As per RFP
35	5.4. Performance Bank Guarantee (PBG)	27	The selected bidder will submit a Performance Bank Guarantee (PBG), within 15 days from the Notification of award, for a value equivalent to 10% of the total order value.	Bidder request to reduce the PBG to 3% of the contract value	As per RFP
36	8.3.2. SLA for Package - II	33	SLA is not capped	Bidder request to cap the SLA for package 2 to 5% of the quarterly invoice value	SLA is Capped for 10% for Quarterly Invoice Value

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
37	20. Payment Terms and Procedure	45	Due Payments shall be made promptly by OCAC, generally within Forty Five (45) days after submission of an invoice and other supporting documents in order.	Bidder request to release the payment within 30days of invoice date	As per RFP
38	20.3. Payment Schedules for Package - II	47	Operation and Maintenance Support : To be released in 10 installments after completion of each 6 months for a period of 5 Years	Bidder request to relase the O&M payment monthly in arrears/Quarterly in advance/Quarterly in arrears	As per RFP
39	21.5.2.2. Specification for Threat Integration Platform	75	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. . has context menu	Bidder request to convert Threat Intelligence sharing platform into onprem Saas Cloud model.	Please refer corrigendum
Firm Name:- **Esquare**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**
1	4. Criteria for Evaluation 4.1. Pre-Qualification (PQ) / Eligibility Criteria 2.Average Sales Turnover	20	Annual average Turnover during any three financial years out of last five financial year ending March – 2023 (as per the last published Balance sheets), should be as follows:	We request you to kindlu reduce the asked turnover for package -II and amend it as Annual average Turnover during any	Clause Amended:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
			a. Package – I - Minimum of Rs. 10 Crores generated from IT Hardware supply and associated maintenance services. b. Package – II - Minimum of Rs. 30 Crores generated from Supply of Security Software Solution.	three financial years out of last five financial year ending March – 2023 (as per the last published Balance sheets), should be as follows: a. Package – I - Minimum of Rs. 10 Crores generated from IT Hardware supply and associated maintenance services. b. Package – II - Minimum of Rs. 10 Crores generated from Supply of Security Software Solution.	
2	4. Criteria for Evaluation 4.1. Pre-Qualification (PQ) / Eligibility Criteria **6.Quality Certifications**	22	Bidder and OEM should have ISO 9001:2015, ISO 20000:2018, ISO 27001:2013 / ISO 27001:2022 Certifications.	Requesting you to kindly ammend this cluase as: Bidder and OEM should have ISO 9001:2015, ISO **20000-1:2018**, ISO 27001:2013 / ISO 27001:2022 Certifications.	Clause Amended:- Please refer corrigendum.
3	5.4. Performance Bank Guarantee (PBG),i.	27	i.The selected bidder will submit a Performance Bank Guarantee (PBG), within 15 days from the Notification of award, for a value equivalent to 10% of the total order value.	Requesting you to kindly ammend this cluase as: i.The selected bidder will submit a Performance Bank Guarantee (PBG), within 15 days from the Notification of award, for a value equivalent to **5%** of the total order value.	As per RFP
4	9.1.3. Project Deliverables, Milestones & Time Schedule	39	Delivery of Equipment: 4 Weeks from date of issue of Purchase Order to the Bidder. Installation, Configuration & Integration: 6 Weeks from date of issue of Purchase Order to the Bidder	Requesting you to ammend this clause as: Delivery of Equipment: **4 to 8 Weeks** from date of issue of Purchase Order to the Bidder. Installation, Configuration & Integration:	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
				2 to 3 Weeks from date of delivery Completion and issue of intimation letter of site readyness.	
5	10.2 Project Deliverables, Milestones & Time Schedule	42	Delivery of Tools: 4 Weeks from date of issue of Purchase Order to the Bidder. Installation, Configuration & Integration: 8 Weeks from date of issue of Purchase Order to the Bidder.	Requesting you to ammend this clause as: **Delivery of Tools:** **4 to 8 Weeks from date of issue of Purchase Order to the Bidder.** **Installation, Configuration & Integration:** **2 to 3 Weeks from date of delivery Completion and issue of intimation letter of site readyness.**	As per RFP
6	21.5.1.2. Specification for 24 Port Layer-2 Managed Switch	57	Switch should have minimum of **12 x 10/100/1000 Mbps RJ45**, 6x1G SFP(MM), 6x10G SFP+(SM) plus 4 x1/10G SFP+ (MM)uplink ports.	Request to please change this as "Switch should have minimum of **12 x 1000 Mbps RJ45**, 6x1G SFP(MM), 6x10G SFP+(SM) plus 4 x1/10G SFP+ (MM)uplink ports.". Request to relax for wider OEM participations.	Clause Amended:- Please refer Corrigendum
7	21.5.1.2. Specification for 24 Port Layer-2 Managed Switch	57	Switch should support network segmentation that overcomes the limitation of VLANs using VXLAN and **VRFs.**	**VRF is not L2 functionality.**Please remove from this clause for wider OEM participations.	Clause Amended:- Please refer Corrigendum
8	21.5.1.2. Specification for 24 Port Layer-2 Managed Switch	57	Switch should support 802.1x authentication and accounting, IPv4 and IPv6 ACLs and Dynamic VLAN assignment and **MACSec-128 on hardware for all ports.**	**MACsec is very OEM speicifc feature practice.**Request to please remove for wider OEM participations.	Clause Amended:- Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
9	21.5.1.2. Specification for 24 Port Layer-2 Managed Switch	57	The OEM must feature in the Leaders segment of the **Gartner Magic Quadrant for Data Center Enterprise** Networking published for last 3 consecutive years	Since 2022 Gartner stopped publishing DC report.Hence request to please consider "The OEM must feature in the Leaders segment of the Gartner Magic Quadrant for **Wired and Wireless networking** published for last 3 consecutive years". Request to please relax for wider OEM participations.	Clause Deleted:- Please refer Corrigendum
10	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should support (DAST) dynamic application security testing. The proposed solution should provide as SaaS offering that is hosted from within India location data centers.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause asks for Saas offering, hence request to please change this point as below The proposed solution should support (DAST) dynamic application security testing. The proposed solution should be deployed on premise with unified/single console for existing Infra Vulnerability management & Web application scanning solution part of this RFP.	Please refer corrigendum
11	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 :- Section :- 21.5.2.3.	81	The proposed solution should propose elastic asset licensing.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
	Specification for Web Application Scanning (WAS) Tool				
12	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution must allow users to scan their RESTful API endpoints by providing a Swagger or OpenAPI specification file.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum
13	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose unified Web App Scanning and Vulnerability Management.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should propose unified console for Web App Scanning procured under this RFP and existing Infra Vulnerability Management Solution.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
14	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should be hosted on the cloud.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should be deplyed on premise.	Please refer corrigendum
15	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should achieve SSAE16 SOC 2 and/or CSA Star certification.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
16	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose cloud and on-prem scanners.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should offers on premise scanners.	Please refer corrigendum
17	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose scanners that managed by the platform, e.g. updates to vulnerability signatures, code, and other updates.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below 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.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
18	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt data at rest - data is stored on encrypted media using at least one level of AES-256 encryption.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum
19	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt data in transit - data is encrypted in transport using TLS v1.2 with a 4096-bit key (this includes internal transports)	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
20	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt sensor communication – Traffic from the sensors to the platform is always initiated by the sensor and is outbound-only over port 443. Traffic is encrypted via SSL communication using TLS 1.2 with a 4096-bit key.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum
21	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support Single sign-on (SSO) authentication methods.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
22	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support Two-Factor Authentication (2FA).	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum
23	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should have disaster recovery procedures and redundancies in place to minimize disruption.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
24	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should service strive to provide a 99.95% or better uptime.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum
25	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should be able to partition/segregate customer data from other users.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
26	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should not access, store, or process any Personally Identifiable Information (PII) or Protected Health Information (PHI).	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum
27	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should have all data in all states in the cloud platform is encrypted with at least one level of encryption, using no less than AES-256.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
28	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should propose unified modern attack surface visibility.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer corrigendum
29	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support the ability to produce reports in the following report formats: Json, CSV, XML.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should support the ability to produce reports in the following report formats: CSV & PDF.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
30	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	License to be Provided No .of FQDNs- Minimum 1000 FQDNs	Sizing Queries:- 1. Please provide the Number of location hosting these applications. 2. Data retention policy for Web application scanning data.	1. Please provide the Number of location hosting these applications- On Premise Solution. Console to be deployed at Central Location and Unlimited Scanner to be placed as per OCAC's requirement 2.Data retention policy for Web application scanning data.- 180 Days

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
31	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 :- Section :- 21.5.2.4. Project Citation Format	85	Project Citation Format	We request to please confirm if project citation can be provided for Saas/on premise deployment for WAS solution, as funtionality of the solution is similar only model of deployment is as per client requirement.	Project Citation can be provided for SaaS/on premise deployment of WAS Solution
32	4.1.6	Page 22	Bidder and OEM should have ISO 9001:2015, ISO 20000:2018, ISO 27001:2013 / ISO 27001:2022 Certifications.	Bidder and OEM should have ISO 9001:2015, ISO 27001:2013 / ISO 27001:2022 Certifications Kindly Remove ISO 20000:2018. The ISO 20000:2018 standard provides organizations with a set of requirements for establishing, implementing, maintaining and continually improving a service management system (SMS) with is not valid for NGFW OEM	Clause Amended:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
33	9.1.iii	on page 38	The implementation of this project is extremely critical for CSOC wherein the entire demographics of the Network/server infrastructure setup are going to be realigned. Hence the bidder is expected to use the services of OEM nominated professional services who will be present and be involved in the critical tasks from day 1(One). The OEM professional services are supposed to impart the following services but not limited to the same.	The implementation of this project is extremely critical for CSOC wherein the entire demographics of the Network/server infrastructure setup are going to be realigned. Hence the bidder is expected to use the services of OEM **Certified** professional services who will be present and be involved in the critical tasks from day 1(One). The OEM professional services are supposed to impart the following services but not limited to the same. Generally Mode of Operation for all OEM is Centrally and Via Channel Partner , therefore requesting for adding OEM/Bidder point SOW Sections	As per RFP
34	9.1.v	on page 38	The OEM shall ensure the seamless installation and integration of the offered solution without disturbing the on-going working of the existing equipment and applications	The **OEM / Bidder** shall ensure the seamless installation and integration of the offered solution without disturbing the on-going working of the existing equipment and applications Generally Mode of Operation for all OEM is Centrally and Via Channel Partner , therefore requesting for adding OEM/Bidder point SOW Sections	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
35	9.1.2.iii	on page 39	The successful bidder will be required to hold administration training for at least 4 Officials / Management team of OCAC by the OEM, covering basic concept, configuring as per the different specs, report generations in different customized formats like time wise, severity wise, protocol wise, source/destination etc., log analysis, definition &software version update/upgrade. The training will be provided on premises at CSOC and OEM has to provide all licenses for the same.	The successful bidder will be required to hold administration training for at least 4 Officials / Management team of OCAC by the **OEM/ OEM Certified Engineer,** covering basic concept, configuring as per the different specs, report generations in different customized formats like time wise, severity wise, protocol wise, source/destination etc., log analysis, definition &software version update/upgrade. The training will be provided on premises at CSOC and **OEM/ Bidde**r has to provide all licenses for the same. Generally Mode of Operation for all OEM is Centrally and Via Channel Partner , therefore requesting for adding OEM/Bidder point SOW Sections	As per RFP
Firm Name:- **PrintLink**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
1.	4.1. Pre-Qualification (PQ) / Eligibility Criteria-point no-02 Average Sales Turnover	20	Annual average Turnover during any three financial years out of last five financial year ending March – 2023 (as per the last published Balance sheets), should be as follows: a. Package – I - Minimum of Rs. 10 Crores generated from IT Hardware supply and associated maintenance services. b. Package – II - Minimum of Rs. 30 Crores generated from Supply of Security Software Solution.	It's essential to highlight that providing the turnover amounts for specific categories, as requested in the RFP, may not be feasible due to the nature of financial reporting. Typically, balance sheets do not segregate revenue generated from specific product or service categories in a manner that aligns directly with the requirements outlined in the RFP.	Clause Amended:- Please refer corrigendum
Firm Name:- **KasperSky**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**
1	Platform	59	A. ISO/IEC 27701:2019 for Privacy Information Management System B. ISO 9001 Compliant Multitenancy	As the Threat Intelligence will be provided to customer, request	No Clarity on Query
2	Platform	59	Platform should provide the UI in multiple languages(Eg.(i) Arabic (ii) Chinese (both simplified and traditional script) (iv) Farsi (Persian) (v) French (vi) German (vii) Japanese (viii) Russian (ix) Spanish (x) English) & support Summarization & translation of the information	Providing the UI in multiple language as mentioned will not be feasible for any OEM. Assume that the reference is for covering the intelligence in the mentioned languages	Clause Amended:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
3	Brand Inteligence	66	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. For image results there should be an option to disable viewing/blurring of images or reporting it.	Image search will limit wider OEM participation	Clause Amended:- Please refer corrigendum
4	Attack Surface Management	68	Platform should discover & then monitor the complete Tech Inventory of customer, including but not limited to: — Cloud Buckets — Domains — IPs — IP Ranges — Subdomains — DNS Records (A, AAAA, CNAME, SOA, MX, NS, TXT etc.) — Digital Certificates — Trackers — Keywords — Technologies — Emails — Executives (Cxx / VPs)	Monitoring Cloud Buckets will be a challenge, kindly consider removing the same and that could be done by active scanner	As per RFP
5		69	Platform should also monitor cloud infrastructure of the customer & provide the visibility of the issues & vulnerabilities. Tool should maintain the dynamic cloud inventory	This point should be achievable by a dedicated vulnerability scanner	Clause Deleted:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
6		69	The Platform must monitor misconfigured cloud repositories, public folders and peer- to-peer networks for data that could represent leaked confidential or sensitive information.	This point should be achievable by a dedicated vulnerability scanner	Clause Deleted:- Please refer corrigendum
7	Browser Extension	72	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 IOCs being shown on the page for reducing triage time for analyst.	Request to consider Browser instead of Browser extension	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
8		72	The browser extension must have capability to block potentially malicious links on the webpage being reviewed by the analyst	Request to consider Browser instead of Browser extension	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
9		72	The browser extension must have the option to enable or disable automatic detection of IOCs like IP, Domain, URL, hash and vulnerability (CVE)	Request to consider Browser instead of Browser extension	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
10		72	The browser extension must work with the following solutions Anomaly ThreatStream, ArcSight ESM, ELK (Dashboard only), MISP, Qualys, The Hive Project, VirusTotal etc	Request to consider Browser instead of Browser extension	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					desired outcome
11		72	The browser extension 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	Request to consider Browser instead of Browser extension	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
12		72	The browser extension must have the capability to upload suspicious file URLs for detonation and analysis to OEM offered sandbox solution	Request to consider Browser instead of Browser extension	The OEM needs to justify and demonstrate how they can perform the IOC

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
13		73	Dynamic Malware Sandboxing should be available: The service should support malware sandboxing by allowing users to a. Upload suspicious files to the platform and download a detailed file behavior analysis report and network analysis report for each uploaded file 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 c. The sandbox should protect organizational privacy by not uploading the file to any publicly accessible repository or third party B. The sandboxing should support operating systems such as Windows, Linux, Mac IoS & Android at a minimum. C. The service should support automated analysis of at-least 50 samples per day D. The service provider should provide analyst support for report interpretation and explanation as and when required.	Kindly consider removing Linux and Mac in Sandbox environment	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
14	Takedown Service	68	Platform should monitor & do a Takedown of the following cases (including but not limited to): - Phishing sites & Campaigns - Fake Mobile Apps on Appstore, Playstore & other 3rd party Application stores - Fake Customer Service Contact details - Fake Social Media profiles - Fake Domains/URLs and Web pages - Fake recruitment drives - Fake Videos or Images using client Logos	Kindly consider removing 3rd Party application store,	Clause Amended:- Please refer corrigendum
15	Pre Qualification/Eligibility Criteria Quality Certification	22	Bidder and OEM should have ISO 9001:2015, ISO 20000:2018, ISO 27001:2013 / ISO 27001:2022 Certifications.	Kindly update to ISO 9001:2015/ ISO 20000:2018/ ISO 27001:2013 / ISO 27001:2022 and as the certification might be under process, request to consider valid recent certificate	Clause Amended:- Bidder/ OEM should have ISO 9001:2015, ISO 27001:2013 / ISO 27001:2022 Certifications.
16		59	The OEM of the solution must provide access to unlimited online training to the offered solution including YARA rules	Kindly consider limiting the training for stipulated number of employees	Training should be provided to 5 No.s of Personnel from OCAC and Unlimited access to OEM LMS.

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
17		59	Incident Response Services (a) On-demand Malware Analysis and Reverse Engineering Assistance (b) On-demand Computer Forensics Analysis, Log Analysis, and Investigation	Kindly consider to mention Incident Reponse service in man hours as this would be the basis and impact commercial	Clause Deleted Please refer Corrigendum
18		60	Platform should support application security scanning of web applications (OWASP Top 10 vulnerabilities) & should provide visibility into Botnet Detection	OWASP top 10 vulnerability scanning would be a dedicated solution and rather a service to check, From Threat Intelligence perspective it will not be covered in general. Consider to remove this point as this is also added in Web Application scanner component	Clause Deleted:- Please refer corrigendum
19	Darkweb & Deepweb Monitoring	60	Bidder should provide an early intelligence on the Compromised endpoints, Cookies & Session keys of customer internal application available for sale in Darkweb Marketplaces	Kindly remove this clause for wider participation	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
20		60	The Platform must be able to create, monitor, automate alert and report for threat on Dark Web but is not limited to, the following: -Employee compromised credentials -Sensitive information Leakage such as Username Password Secret token access keys -Compromised PII such as Email ID, Phone number and Address. -information about the compromised system such as device ID, host name, IP address etc to help in forensic investigation -Malware and Malicious Infrastructure related to Customer domain -Private / Sensitive Documents relating to the business. -Hacking documents/tools specifically targeting client; -Leaked Source Code. -Intellectual property exposed or leaked -Copyright / Trademark infringement. -Technical Information / Data that could be used to compromise corporate systems. - Mentions of IP Addresses and Infrastructure -Use of BIN and other PII serial numbers to identify client-related accounts and credentials. -Stolen / Compromised Login Credentials and Customer Account Information. - Exposure in 3rd Party Breaches	Kindly consider to remove the below -Private / Sensitive Documents relating to the business. -Intellectual property exposed or leaked -Copyright / Trademark infringement.	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
21		60	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. For image results there should be an option to disable viewing/blurring of images or reporting it.	Kindly remove this clause for wider participation	Clause Amended:- Please refer corrigendum
22		61	Platform should provide intelligence from Internet traffic analysis to look for possible exfiltration or C2 extraction from OCAC PUBLIC IP range	Kindly remove this clause for wider participation	As per RFP
23		61	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	Kindly remove this clause for wider participation	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
24	Brand Intelligence	61	Social Media Monitoring: The platform should monitor all the major social media platform, including, but not limited to; Twitter, Facebook, YouTube, Instagram, LinkedIn, Tiktok,Vimeo, RSS All data sources should be collectively analyzed 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.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	Kindly remove this clause for wider participation	Clause Amended:- Please refer corrigendum
25	Brand Intelligence	61	Platform should provide : Website Watermarking Website Defacement monitoring	Kindly remove this clause for wider participation	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
26	Brand Intelligence	61	The Bidder/OEM should be member of International Anti-Phishing Working Group (APWG). Solution should provide the visibility of DNS records, Whois records, MX records, screenshot tagged to a typoquatted domain Solution should provide Domain Watclisting feature, to get instant alert whenever there's a change in the status of domain Platform should be capable of doing Image/Logo monitoring to identify profile impersonation Finding domains and emails mentions on Code Repository websites like Github etc CXOs fake social media profiles, posts, pages and groups, takedown is also expected here	Kindly remove this clause for wider participation	Clause Amended:- Please refer corrigendum
27	Brand Intelligence	61	Platform should monitor & do a Takedown of the following cases (including but not limited to): - Phishing sites & Campaigns - Fake Mobile Apps on Appstore, Playstore & other 3rd party Application stores - Fake Customer Service Contact details - Fake Social Media profiles - Fake Domains/URLs and Web pages - Fake recruitment drives - Fake Videos or Images using client Logos	Kindly remove this clause for wider participation	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
28	Attack Surface management	63	Platform should also monitor cloud infrastructure of the customer & provide the visibility of the issues & vulnerabilities. Tool should maintain the dynamic cloud inventory	Kindly remove this clause for wider participation	Clause Deleted:- Please refer corrigendum
29	Attack Surface management	63	The Platform must monitor misconfigured cloud repositories, public folders and peer- to-peer networks for data that could represent leaked confidential or sensitive information.	Kindly remove this clause for wider participation	Clause Deleted:- Please refer corrigendum
30	Attack Surface management	67	Platform should monitor exposed sensitive codes on all of the platforms listed below:(Not Limited to) Github BitBucket Postman Docker Hub	Kindly remove this clause for wider participation	As per RFP
31	Attack Surface management	67	Bidder should Provide Public Assets information's like(Not Limited to) *Screenshot *Web Applications details *WAF and CDN Information *Favicon Detect -Vulnerabilities and Critical Open -Virtual Host (Shadow IT Asset) - Local file inclusion -Path Traversal - Default Logins - Web App Misconfigurations - Insecure Design - Broken Authentication	Kindly remove this clause for wider participation	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
32	Attack Surface management	67	The solution should show information about spam attacks in which the requested object is attached to email messages.	Kindly remove this clause for wider participation	Clause Deleted Please refer Corrigendum
33	Attack Surface management	68	Platform should support application security scanning of web applications (OWASP Top 10 vulnerabilities) & should provide visibility into Botnet Detection	Kindly remove this clause for wider participation	Clause Deleted:- Please refer corrigendum
34	Attack Surface management	69	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 a) New critical vulnerability announcement and real-world risk of the vulnerability at Pre-NVD level. b) Trending Vulnerabilities in specific Industries c) Vulnerabilities exploited in the wild by Malwares d) CVEs with low, medium or high potential for exploitation. e) Exploitation has been reported or confirmed to widely occur.	Kindly remove this clause for wider participation	As per RFP
35		70	The vulnerability threat intelligence should be bundled with tools to import vulnerability scan results in CSV format	Kindly remove this clause for wider participation	As per RFP
36		70	The vulnerability solution must have a dashboard view that identifies all types of vulnerabilities with a risk and exploit rating	Kindly remove this clause for wider participation	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
37		70	The solution must have option to restrict view of cleartext password for limited admin users only	Kindly remove this clause for wider participation	As per RFP. If the Role Based access control suffice the requirement of RFP then it is acceptable
38	Support	72	Professional Service a) Full-time/ part-time “named” threat intelligence analyst services for threat intelligence operations support b) Daily/Weekly Alert Summary and Monthly Executive Summary Reports (if required) c) On-demand Analyst services for threat research and investigations and custom reports	Kindly remove this clause for wider participation	As per RFP
39	Threat Intel Sharing Platform Capabilities	75	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	Kindly remove this clause for wider participation	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
40	Threat Intel Sharing Platform Capabilities	75	The solution should be integrated with at least 2 OSINT feeds and 1 commercial feeds/risk lists(not in scope of TIP vendor) 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.	Kindly remove this clause for wider participation	Please refer corrigendum
41	Threat Intel Sharing Platform Capabilities	76	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	Kindly remove this clause for wider participation	Please refer corrigendum
42	Threat Intel Sharing Platform Capabilities	76	The offered solution must provide threat feed integration with Checkpoint and Fortinet make NGFW, Trend Micro make EDR/AV, McAfee Web Gateway and McAfee 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 min 30 man days for future customization and integrations	Kindly remove this clause for wider participation	Please refer corrigendum
43	Threat Intel Sharing Platform Capabilities	76	The platform should support Threat Intelligence Collection, Evaluation, Ingestion, Processing, Translation, Prioritization, Integration & Aggregation and real time Dissemination.	Kindly remove this clause for wider participation	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
44	Threat Intel Sharing Platform Capabilities	76	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.	Kindly remove this clause for wider participation	Please refer corrigendum
45	Threat Intel Sharing Platform Capabilities	77	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	Kindly remove this clause for wider participation	Please refer corrigendum
46	Threat Intel Sharing Platform Capabilities	77	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.	Kindly remove this clause for wider participation	Please refer corrigendum
47	Threat Intel Sharing Platform Capabilities	77	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	Kindly remove this clause for wider participation	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
48	Threat Intel Sharing Platform Capabilities	77	The solution should provide for advanced filtering functionalities and warning list to help the analysts to contribute events and attributes.	Kindly remove this clause for wider participation	Please refer corrigendum
49	Threat Intel Sharing Platform Capabilities	77	The solution should provide options for analyst to collaborate on events and attributes to propose changes or updates to attributes/indicators.	Kindly remove this clause for wider participation	Please refer corrigendum
50	Threat Intel Sharing Platform Capabilities	77	should be integrated from day one for OCAC to provide feeds like C2 communicating IPs, 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	Kindly remove this clause for wider participation	Please refer corrigendum
51	Threat Intel Sharing Platform Capabilities	77	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 organizations.	Kindly remove this clause for wider participation	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
52	Threat Intel Sharing Platform Capabilities	78	The solution must have integrated encryption and signing of the notifications via PGP and/or S/MIME depending of the user preferences.	Kindly remove this clause for wider participation	Please refer corrigendum
53	Threat Intel Sharing Platform Capabilities	78	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.	Kindly remove this clause for wider participation	Please refer corrigendum
54	Support		The solution must include Dedicated or shared intelligence analyst from OEM for continuous product usage support and regular reviews	Kindly remove this clause for wider participation	As per RFP
Firm Name:- **Reliance Jio**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**
1	10. Details on Scope of Work for Package - II	41	Solution should be easily integrated with existing SIEM solution of CSOC.	Requesting OCAC to provide clarification on what is the current SIEM tool that is deployed. Also request OCAC to share tentative EPS count which would require to be managed by the bidder.	The current SIEM is in the Year 2022 0f Magic Quadrant
2	10. Details on Scope of Work for Package - II	41	Solution should be easily integrated with existing SIEM solution of CSOC.	Please share the format (extension of the files) which is required by existing SIEM to integarate the Threat Intelligence solution	As per Industry Standard

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
3	8.3.2. SLA for Package - II	34	0.5 % Cost of Tool Value deducted from O&M Cost	Requesting OCAC to reduce the penalties for all the listed SLAs as the penalties are very high.	As per RFP
4	21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should provide as SaaS offering that is hosted from within India location data centers.	Please clarify if the Web Application Scanning tool required is a Cloud tool or On-prem tool.	Clause Amended Please refer Corrigendum
5	10.3. Indicative Bill of Quantity (BOQ)	42	Web Application Scanning Tool	Please provide the number of in Scope applications Please provide the number of concurrent scan Please provide the number of end user licences required.	Centralised On-premises Solution Required. Scanner to be deployed as per OCAC's Requirement
6	21.5.2.1.Specification for Threat Intel Solution	74	The solution must be provided with 24/7 access to the support team via web, email and phone	Request OCAC to clarify if the security services can be provisioned using the state of the art managed security services of the bidder in remote shared model.	Security services can be provisioned using the state of the art managed security services of the bidder in remote shared model.

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
7	10.3 Indicative Bill of Quantity (BOQ) 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	42 81	Web Application Vulnerability Scanning tool should be On – Premises Deployment **And** The proposed solution should be hosted on the cloud.	The controversal statement made for Web Appliction Scanning tool. In section 10.3 mentioned that it should be on-premises deployment but in 21.5.2.3 section mentioned that it should be hosted on the cloud. Need the clarification on it?	It's an on-premises deployment Please refer Corrigendum
	20.3. Payment Schedules for Package - II	46	The overall payment % schedule provided for 90% of the amount instead of 100%	The overall payment % schedule provided for 90% of the amount instead of 100%	Clause Amended Please refer Corrigendum
	10.2 Operation & Maintenance (O&M)	42	O&M period will start after successful completion of Installation, Configuration & Integration	Is O & M support 24X7 required? Support time lines not mentioned in the RFP, please calrify it.	We have mentioned the support in 22.5.2 (Sl.No.15)
8	9.1.3. Project Deliverables, Milestones & Time Schedule	39	1.Delivery of Equipment : 4 Weeks from date of issue of Purchase Order to the Bidder 2.Installation, Configuration & Integration: 6 Weeks from date of issue of Purchase Order to the Bidder	1.Please increase The timelines for delivery of equipment to 12 to 16 weeks 2.Please provide 4 weeks timeline post delivery for Installationation, configuration & integration	As per RFP
9	21.5.1.1. Specification for Firewall	54	1RU Firewall with 70 Gbps throughput support.	1RU firewall device with 70 Gbps throughput isn't readily offered by most vendors. Kindly change to 2RU.	As per RFP
10	21.5.1.2.Specification for 24 Port Layer-2 Managed Switch	57	Switch should support min 16K MAC addresses and min 1000 active VLANs. The switch should support the network segmentation that overcomes the	Layer 2 managed switches generally lack support for VXLAN. You may need to consider relaxing this requirement or opting for a Layer 3 switch instead.	Clause Amended Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
			limitation of VLANs using VXLAN and VRFs.		
11	4.1. Pre-Qualification (PQ) / Eligibility Criteria	20	Annual average Turnover during any three financial years out of last five financial year ending March – 2023 (as per the last published Balance sheets), should be as follows: a. Package – I - Minimum of Rs. 10 Crores generated from IT Hardware supply and associated maintenance services. b. Package – II - Minimum of Rs. 30 Crores generated from Supply of Security Software Solution.	Request to Amend as: Annual average Turnover during any three financial years out of last five financial year ending March – 2023 (as per the last published Balance sheets), should be as follows: a. Package – I - Minimum of Rs. 10 Crores generated from IT**/ITES** ~~Hardware supply~~ and associated maintenance services. b. Package – II - Minimum of Rs. 30 Crores generated from **IT/ITES Services** ~~Supply of Security Software Solution.~~	Clause Amended:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
12	8.1.1. Right to Terminate the Process	30	OCAC reserves the right to cancel the contract placed on the selected bidder and recover expenditure incurred by OCAC under the following circumstances: - i. The selected bidder commits a breach of any of the terms and conditions of the bid. ii. The bidder goes into liquidation, voluntarily or otherwise. iii. If the selected bidder fails to complete the assignment as per the timelines prescribed in the RFP and the extension if any allowed, it will be a breach of contract. OCAC reserves its right to cancel the order in the event of delay and forfeit the bid security as liquidated damages for the delay. iv. In case the selected bidder fails to deliver the quantity as stipulated in the delivery schedule, OCAC reserves the right to procure the same or similar product from alternate sources at the risk, cost and responsibility of the selected bidder, after 2 weeks of cure period. v. OCAC reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking the bank guarantee under this contract.	**Seek deletion of subclause (iv) regarding failure to deliver the quantity as LD is already agreed, an additional cost is excessive**. OCAC reserves the right to cancel the contract placed on the selected bidder and recover expenditure incurred by OCAC under the following circumstances: - i. The selected bidder commits a breach of any of the terms and conditions of the bid. ii. The bidder goes into liquidation, voluntarily or otherwise. iii. If the selected bidder fails to complete the assignment as per the timelines prescribed in the RFP and the extension if any allowed, it will be a breach of contract. OCAC reserves its right to cancel the order in the event of delay and forfeit the bid security as liquidated damages for the delay. iv. OCAC reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking the bank guarantee under this contract.	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
13	8.4. Dispute Resolution Mechanism	35	iii. In case, it is not resolved between OCAC and the bidder, it will be referred to Principal Secretary to Govt., E&IT Department., Govt. of Odisha for negotiation and his decision would be final and binding for both the parties.	Seek deletion of subclause (iii) as such a call extinguishes the right to take any particular dispute to Arbitration.	As per RFP
14	10. Details on Scope of Work for Package – II	41	Query	What is the end of life and end of support life policy?	The End of Support of the Product should be under our Warranty Period
15	11. Right to alter Quantities	42	OCAC reserves the right to give repeat order to the L1/H1 bidder in Respective Package for maximum upto 20% of ordered quantity, if required, within the tender validity period of 180 days from the last date of submission of bid under same terms and conditions with same Specifications and Rate. Any decision of OCAC in this regard shall be final, conclusive and binding on the bidder. If OCAC does not purchase any of the tendered articles or purchases less than the quantity indicated in the bidding document, the bidder(s) shall not be entitled to claim any compensation.	**Request the clause to be amended as follows:** OCAC reserves the right to give repeat order to the L1/H1 bidder in Respective Package for maximum upto 20% of ordered quantity, if required, within the tender validity period of 180 days from the last date of submission of bid under same terms and conditions with same Specifications and Rate. If OCAC does not purchase any of the tendered articles or purchases less than the quantity indicated in the bidding document, the bidder(s) shall not be entitled to claim any compensation.	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
16	17. Limitation of Liability	44	Except in cases of gross negligence or willful misconduct: - a. neither party shall be liable to the other party for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the supplier/ selected bidder to pay liquidated damages to the Purchaser; and b. the aggregate liability of the selected bidder to the Purchaser, whether under the Contract, in tort, or otherwise, shall not exceed the amount specified in the Contract, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the supplier/ selected bidder(s) to indemnify the Purchaser with respect to patent infringement.	**Request addition in the clause as follows:** Except in cases of gross negligence or willful misconduct: - a. neither party shall be liable to the other party for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the supplier/ selected bidder to pay liquidated damages to the Purchaser; and b. the aggregate liability of the selected bidder to the Purchaser, whether under the Contract, in tort, or otherwise, shall not exceed the amount specified in the Contract, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment **manufactured by the selected bidde**r, or to any obligation of the supplier/ selected bidder(s) to indemnify the Purchaser with respect to patent infringement **claimed by a third party.**	As per RFP
18	10. Details on Scope of Work for Package - II	41	Solution should be easily integrated with existing SIEM solution of CSOC.	Requesting OCAC to provide clarification on what is the current SIEM tool that is deployed. Also request OCAC to share tentative EPS count which would require to be managed by the bidder.	Repeated Query

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
19	10. Details on Scope of Work for Package - II	41	Solution should be easily integrated with existing SIEM solution of CSOC.	Please share the format (extension of the files) which is required by existing SIEM to integarate the Threat Intelligence solution	Repeated Query
20	8.3.2. SLA for Package - II	34	0.5 % Cost of Tool Value deducted from O&M Cost	Requesting OCAC to reduce the penalties for all the listed SLAs as the penalties are very high.	Repeated Query
21	21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should provide as SaaS offering that is hosted from within India location data centers.	Please clarify if the Web Application Scanning tool required is a Cloud tool or On-prem tool.	Repeated Query
22	10.3. Indicative Bill of Quantity (BOQ)	42	Web Application Scanning Tool	Please provide the number of in Scope applications Please provide the number of concurrent scan Please provide the number of end user licences required.	Repeated Query
23	21.5.2.1.Specification for Threat Intel Solution	74	The solution must be provided with 24/7 access to the support team via web, email and phone	Request OCAC to clarify if the security services can be provisioned using the state of the art managed security services of the bidder in remote shared model.	Repeated Query
24	10.3 Indicative Bill of Quantity (BOQ) 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	42 81	Web Application Vulnerability Scanning tool should be On – Premises Deployment **And** The proposed solution should be hosted on the cloud.	The controversal statement made for Web Appliction Scanning tool. In section 10.3 mentioned that it should be on-premises deployment but in 21.5.2.3 section mentioned that it should be hosted on the cloud. Need the clarification on it?	Repeated Query
	20.3. Payment Schedules for Package - II	46	The overall payment % schedule provided for 90% of the amount instead of 100%	The overall payment % schedule provided for 90% of the amount instead of 100%	Repeated Query

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
	10.2 Operation & Maintenance (O&M)	42	O&M period will start after successful completion of Installation, Configuration & Integration	Is O & M support 24X7 required? Support time lines not mentioned in the RFP, please calrify it.	Repeated Query
25	9.1.3. Project Deliverables, Milestones & Time Schedule	39	1.Delivery of Equipment : 4 Weeks from date of issue of Purchase Order to the Bidder 2.Installation, Configuration & Integration: 6 Weeks from date of issue of Purchase Order to the Bidder	1.Please increase The timelines for delivery of equipment to 12 to 16 weeks 2.Please provide 4 weeks timeline post delivery for Installationation, configuration & integration	Repeated Query
26	21.5.1.1. Specification for Firewall	54	1RU Firewall with 70 Gbps throughput support.	1RU firewall device with 70 Gbps throughput isn't readily offered by most vendors. Kindly change to 2RU.	Repeated Query
	21.5.1.2.Specification for 24 Port Layer-2 Managed Switch	57	Switch should support min 16K MAC addresses and min 1000 active VLANs. The switch should support the network segmentation that overcomes the limitation of VLANs using VXLAN and VRFs.	Layer 2 managed switches generally lack support for VXLAN. You may need to consider relaxing this requirement or opting for a Layer 3 switch instead.	Repeated Query
	4.1. Pre-Qualification (PQ) / Eligibility Criteria	20	Annual average Turnover during any three financial years out of last five financial year ending March – 2023 (as per the last published Balance sheets), should be as follows: a. Package – I - Minimum of Rs. 10 Crores generated from IT Hardware supply and associated maintenance services. b. Package – II - Minimum of Rs. 30 Crores generated from Supply of Security Software Solution.	Request to Amend as: Annual average Turnover during any three financial years out of last five financial year ending March – 2023 (as per the last published Balance sheets), should be as follows: a. Package – I - Minimum of Rs. 10 Crores generated from IT**/ITES** ~~Hardware supply~~ and associated maintenance services. b. Package – II - Minimum of Rs. 30 Crores generated from **IT/ITES**	Repeated Query

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
				Services ~~Supply of Security Software Solution.~~	

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
27	8.1.1. Right to Terminate the Process	30	OCAC reserves the right to cancel the contract placed on the selected bidder and recover expenditure incurred by OCAC under the following circumstances: - i. The selected bidder commits a breach of any of the terms and conditions of the bid. ii. The bidder goes into liquidation, voluntarily or otherwise. iii. If the selected bidder fails to complete the assignment as per the timelines prescribed in the RFP and the extension if any allowed, it will be a breach of contract. OCAC reserves its right to cancel the order in the event of delay and forfeit the bid security as liquidated damages for the delay. iv. In case the selected bidder fails to deliver the quantity as stipulated in the delivery schedule, OCAC reserves the right to procure the same or similar product from alternate sources at the risk, cost and responsibility of the selected bidder, after 2 weeks of cure period. v. OCAC reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking the bank guarantee under this contract.	**Seek deletion of subclause (iv) regarding failure to deliver the quantity as LD is already agreed, an additional cost is excessive**. OCAC reserves the right to cancel the contract placed on the selected bidder and recover expenditure incurred by OCAC under the following circumstances: - i. The selected bidder commits a breach of any of the terms and conditions of the bid. ii. The bidder goes into liquidation, voluntarily or otherwise. iii. If the selected bidder fails to complete the assignment as per the timelines prescribed in the RFP and the extension if any allowed, it will be a breach of contract. OCAC reserves its right to cancel the order in the event of delay and forfeit the bid security as liquidated damages for the delay. iv. OCAC reserves the right to recover any dues payable by the selected Bidder from any amount outstanding to the credit of the selected bidder, including the pending bills and/or invoking the bank guarantee under this contract.	Repeated Query

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
	8.4. Dispute Resolution Mechanism	35	iii. In case, it is not resolved between OCAC and the bidder, it will be referred to Principal Secretary to Govt., E&IT Department., Govt. of Odisha for negotiation and his decision would be final and binding for both the parties.	Seek deletion of subclause (iii) as such a call extinguishes the right to take any particular dispute to Arbitration.	Repeated Query
	10. Details on Scope of Work for Package – II	41	Query	What is the end of life and end of support life policy?	Repeated Query
28	11. Right to alter Quantities	42	OCAC reserves the right to give repeat order to the L1/H1 bidder in Respective Package for maximum upto 20% of ordered quantity, if required, within the tender validity period of 180 days from the last date of submission of bid under same terms and conditions with same Specifications and Rate. Any decision of OCAC in this regard shall be final, conclusive and binding on the bidder. If OCAC does not purchase any of the tendered articles or purchases less than the quantity indicated in the bidding document, the bidder(s) shall not be entitled to claim any compensation.	**Request the clause to be amended as follows:** OCAC reserves the right to give repeat order to the L1/H1 bidder in Respective Package for maximum upto 20% of ordered quantity, if required, within the tender validity period of 180 days from the last date of submission of bid under same terms and conditions with same Specifications and Rate. If OCAC does not purchase any of the tendered articles or purchases less than the quantity indicated in the bidding document, the bidder(s) shall not be entitled to claim any compensation.	Repeated Query

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
29	17. Limitation of Liability	44	Except in cases of gross negligence or willful misconduct: - a. neither party shall be liable to the other party for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the supplier/ selected bidder to pay liquidated damages to the Purchaser; and b. the aggregate liability of the selected bidder to the Purchaser, whether under the Contract, in tort, or otherwise, shall not exceed the amount specified in the Contract, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the supplier/ selected bidder(s) to indemnify the Purchaser with respect to patent infringement.	**Request addition in the clause as follows:** Except in cases of gross negligence or willful misconduct: - a. neither party shall be liable to the other party for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the supplier/ selected bidder to pay liquidated damages to the Purchaser; and b. the aggregate liability of the selected bidder to the Purchaser, whether under the Contract, in tort, or otherwise, shall not exceed the amount specified in the Contract, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment **manufactured by the selected bidde**r, or to any obligation of the supplier/ selected bidder(s) to indemnify the Purchaser with respect to patent infringement **claimed by a third party.**	Repeated Query
30	21.5.2.1. Specification for Threat Intel Solution	68	6 Take Down Service	Please clarify if Take Down Service is a mandatory requirement as it is asked in 21.8.3. Form 9: Financial Proposal Package – II Price discovery section and in the compliance section. If it is mandatory then request OCAC to	It is already clarified in the RFP pg. 92

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
				include take down service in the commercial BOQ.	
Firm Name:- **Inspira**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**
1	21.5.1.1. Specification for Firewall 1.8	54	The appliance should have minimum internal storage of 400 GB SSD for Logs & Reports or better.	Kindly Amend to:The appliance should have minimum internal storage of 1TB SSD for Logs & Reports or better.As it is OEM specific point, for longer period of storing logs we suggest to have separate Syslog server.	It's already mentioned the RFP about that "The appliance should have minimum internal storage of 1TB SSD for Logs & Reports or better."
2	21.5.1.1. Specification for Firewall 3.4	55	The appliance should have minimum Antivirus Throughput of 12 Gbps or better	Kindly remove this clause:This ia OEM specific point, not published by all Firewall OEM. Request you to amend the clause as " The appliance should have minimum 10 Gbps of Threat Prevention Throughput measured with Firewall, IPS, Application Control, and Malware Protection enabled, Enterprise Mix traffic" this point to make this generic so that all leaders OEM can participate.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
3	21.5.1.1. Specification for Firewall 3.6	55	The appliance should have minimum Firewall IMIX Throughput of 28 Gbps or better	Kindly remove this clause:This is not standard parametrs published by all OEMs.	IMIX throughput consideration of Real World/Prod Performance Under Test Condition in Gbps. The IMIX throughput in Data Centre firewall require to handle a large volume of diverse traffic, including network/server access of datacentre. This is in generic requirement/parameter which is available with most of firewall OEM's.

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
4	21.5.1.1. Specification for Firewall 3.8	55	The appliance should have minimum 40000 Number of IPSec VPN Peers supported (Site to Site)	Kindly Amend to:The appliance should have 2000 numbers of IPSEC VPN Peers supported (Site to Site).As OEM specific point and 40,000 Site to Site VPN support with only 13 Gbps of VPN throughput asked in the point no. 3.7 is not matching.	Please refer corrigendum
5	21.5.1.1. Specification for Firewall 3.11	55	The appliance should have minimum 20M Concurrent Session/Concurrent Connection	Kindly amend to:The appliance should have minimum 5 million Concurrent Session/Concurrent Connection.As 20 Million concurrent session/ concurrent connections is too high considering only 500K new sessions per second and considering others performance parameters. Hence we request you to amend the clauses as "The appliance should have minimum 5 million Concurrent Session/Concurrent Connection"	Any traffic session hitting the Data Centre network/server is unpredictable, So higher Concurrent sessions required to scale and accommodate the growing number of devices and users accessing the network in Data Centre. Higher concurrent session/concurrent connection

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					require to process high volume of traffic in the event of DOS/DDOS attacks, security events, and anomalies, which cause surge of concurrent sessions and prevent / hamper connection of data centre Hence, there is a requirement of high concurrent connections in data Centre firewall.

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
6	21.5.1.1. Specification for Firewall 3.14	55	The appliance Should support 25000+ IPS Signature for future upgradation of Next generation IPS license	Kindly Amend to:The appliance should have support 10,000 + IPS signature and support for custom IPS signature creation.As Not all OEMs support the asked parameters, request you to amend the clause as "The appliance should have support 10,000 + IPS signature and support for custom IPS signature creation." to ensure maximum particiaption.	Higher number of IPS signatures increase the breadth of threat coverage and actively blocking potentially malicious traffic based on signatures. Since asked 25000+ signatures are available with majority of the OEM and there is no requirement of custom IPS signatures. Since OEM tested IPS signatures are more reliable and secure than custom signatures.

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
7	9.1.3. Project Deliverables, Milestones & Time Schedule	39	1. Delivery of Equipment: 4 Weeks from date of issue of Purchase Order to the Bidder	Kindly amend as follows: 1. Delivery of Equipment: 6 Weeks from date of issue of Purchase Order to the Bidder	As per RFP
			2. Installation, Configuration & Integration: 6 Weeks from date of issue of Purchase Order to the Bidder	2. Installation, Configuration & Integration: 8 Weeks from date of issue of Purchase Order to the Bidder	As per RFP
			3. UAT, Sign-off: 8 Weeks from date of issue of Purchase Order to the Bidder	3. UAT, Sign-off: 10 Weeks from date of issue of Purchase Order to the Bidder	As per RFP
			4. Training (Knowledge Transfer): Within 10 Weeks from date of issue of Purchase Order to the Bidder	4. Training (Knowledge Transfer): Within 12 Weeks from date of issue of Purchase Order to the Bidder	As per RFP
8	21.5.1. PACKAGE-I 21.5.1.1. Specification for Firewall	56	6. The product shall comply minimum 60% and Above Local content or higher.	As no reputable OEM for Enterprise Firewall/NGFW have MII Class I/II compliance, hence we request you to kindly delete this clause.	Please refer corrigendum
9	21.5.1. PACKAGE-I 21.5.1.2. Specification for 24 Port Layer-2 Managed Switch	57	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 and MACSec-128 on hardware for all ports.	Typically MACSec is available on uplink ports, hence we request the clause to be amended as: "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 and MACSec-128 in hardware for all 1G SFP, 10G SFP+ 40G QSFP+ uplink ports."	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
10	21.5.1. PACKAGE-I 21.5.1.2. Specification for 24 Port Layer-2 Managed Switch	57	8. Should support 8 queues per port and security protocols like RADIUS, TACACS/TACACS+, AAA & SSH. **Always-on POE to that supplies POE power even during schedule reboot.**	While in clause 9 of the specification, it is mandated that the The OEM must feature in the Leaders segment of the Gartner Magic Quadrant for Data Center Enterprise Networking, we wish to bring to your attention that typically in DC switching, PoE as per IEEE 802.3af / 802.3at / 802.3bt are used. Kindly clarify whether PoE is required and if not, kindly amend the clause to remove the PoE requirement.	Please refer corrigendum
11	21.5.1. PACKAGE-I 21.5.1.2. Specification for 24 Port Layer-2 Managed Switch	57	11. Equipment should be minimum TEC certified or IPV6 Ready Logo Certified. IPV6 Routing & Management features should be active from Day-1.	The IPv6 Ready Logo certification is available with only a specific OEM. Request relaxation of the IPv6 Ready logo requirement to ensure broader participation from OEMs which feature in Gartner's Leader quadrant for DC Networking.	As per RFP
12	5.4. Performance Bank Guarantee (PBG)	27	The selected bidder will submit a Performance Bank Guarantee (PBG), within 15 days from the Notification of award, for a value equivalent to 10% of the total order value	Kindly amend PBG it to 3% as per PBG notification from Ministry of Finance where existing 5-10% PBG has been relaxed	As per RFP
13	4. Criteria for Evaluation 4.1. Pre-Qualification (PQ) / Eligibility Criteria	19	Annual average Turnover during any three financial years out of last five financial year ending March – 2023 (as per the last published Balance sheets), should be as follows: a. Package – I - Minimum of Rs. 10 Crores generated from IT Hardware supply and associated maintenance services. b.	Kindly include Supporting document Extracts from the audited Balance sheet and Profit & Loss;OR Certificate from the statutory auditor/Company Secretary/CA	Clause Amended:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
			Package – II - Minimum of Rs. 30 Crores generated from Supply of Security Software Solution.		
14	4. Criteria for Evaluation 4.1. Pre-Qualification (PQ) / Eligibility Criteria	19	The OEM should have implemented at least 5 heterogeneous setups (means BFSI, Government /PSU/Autonomous body).	Kindly Amend it to :The Bidder should have implemented at least 5 heterogeneous setups (means BFSI, Government /PSU/Autonomous body) as it will help to evealuate Bidder capability	As per RFP
15	4.2.2. Technical Evaluation Criteria for Package – II	23	Bidder/OEM should have experience in Threat Intel Solution for SOC environment as per functionalities of Threat Intel Platform Mentioned in RFP - Section 21.5.2.1	Kindly Amend it to: Bidder should have experience in Threat Intel Solution for SOC environment as per functionalities of Threat Intel Platform Mentioned in RFP - Section 21.5.2.1 as it will help to evealuate Bidder capability	As per RFP
16	4.2.2. Technical Evaluation Criteria for Package – II	23	Bidder/OEM should have experience in Threat Integration Platform for SOC environment as per functionalities of Threat Integration Platform entioned in RFP - Section 21.5.2.2	Kindly Amend it to:Bidder should have experience in Threat Integration Platform for SOC environment as per functionalities of Threat Integration Platform entioned in RFP - Section 21.5.2.2 as it will help to evealuate Bidder capability	As per RFP
17	4.2.2. Technical Evaluation Criteria for Package – II	23	Bidder/OEM should have experience in Supply, Installation and Support of Web Scanning Tool for Data CentreSection 21.5.2.3	Kindly Amend it to:Bidder/OEM should have experience in Supply, Installation and Support of Web Scanning Tool for Data CentreSection 21.5.2.3 as it will help to evealuate Bidder capability	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
18	10.Details on Scope of Work for Package - II	41	General Querry	Clarification Required: A. Who is going to manage the day-to-day operation of the proposed solution @OCAC SOC ? B. Dose customer have the qualified resources to operate the solution of Package-II - Threat Intel Solution - Web Application Scan (DAST) Tool C. Or dose the bidder also needs to supply onsite engineer for managing the supplied solutions at OCAC premises for the entire duration of the project for 5 years. - If Yes, please share the total Nos. of resources required (L1,L2 and L3) with details of Roles and Responsibilities and Minimum Qualification and Experience. - And the Duty Time/hrs of the Resources in a week	A. It will be managed by CSOC B. OEM has to impart training to CSOC personnel for usability of Tool and provide support C. Based on the nature of requirement it's upto Bidder to provide the support.
19	21.5.2. PACKAGE-II	59	General Querry	Dose the bidder need to implement the solution in High Availability ?	It's Bidder/OEM to provide the solution

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
20	21.5.2.3.Specification for Web Application Scanning (WAS) Tool	81	General Querry	will OCAC accept an On-prem solution or its only SaaS acceptable	On-prem Solution
21	21.5.2.3.Specification for Web Application Scanning (WAS) Tool	84	License to be Provided No .of FQDNs-Minimum 1000 FQDNs	Does the bidder need to supply and deploy the WAS Tool with capacity of 1000 FQDN licenses from Day-1 ?	Yes, After Successful completion of Tool Installation and Configuration
22	21.5.2.1. Specification for Threat Intel Solution 21.5.2.2. Specification for Threat Integration Platform	59 and 75	General Querry	This proposed solution for providing Threat Intel Platform, Threat Intel Feeds and Deep and Darkweb & Deepweb Monitoring should be same OEM. Or Will OCAC accept different OEM's also for Threat Intel Platform, Threat Intel Feeds and Deep and Darkweb & Deepweb Monitoring ?	Bidder/OEM has to provide the solution considering ease of usability
23	21.5.2.4.Project Citation Format	85	General Querry	Please Clarify : Is the Citation required to be submitted by the bidder or OEM. If it is only meant for Bidder to submit then the project is only specific/restricted to WAS and Threat Intel solutions ? Or can also be a multi-security project where both solution are part of the	Is the Citation required to be submitted by the bidder or OEM. Ans- Both Bidder/OEM experience will suffice

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
				Solution BoQ supplied in BFSI/PSU/Gov/Enterprise organisation.	
24	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should support (DAST) dynamic application security testing. The proposed solution should provide as SaaS offering that is hosted from within India location data centers.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause asks for Saas offering, hence request to please change this point as below The proposed solution should support (DAST) dynamic application security testing. The proposed solution should be deployed on premise with unified/single console for existing Infra Vulnerability management & Web application scanning solution part of this RFP.	Please refer Corrigendum
25	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose elastic asset licensing.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
26	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution must allow users to scan their RESTful API endpoints by providing a Swagger or OpenAPI specification file.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
27	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose unified Web App Scanning and Vulnerability Management.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should propose unified console for Web App Scanning procured under this RFP and existing Infra Vulnerability Management Solution.	Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
28	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should be hosted on the cloud.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should be deplyed on premise.	Please refer Corrigendum
29	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should achieve SSAE16 SOC 2 and/or CSA Star certification.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
30	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose cloud and on-prem scanners.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should offers on premise scanners.	Please refer Corrigendum
31	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose scanners that managed by the platform, e.g. updates to vulnerability signatures, code, and other updates.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below 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.	Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
32	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt data at rest - data is stored on encrypted media using at least one level of AES-256 encryption.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
33	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt data in transit - data is encrypted in transport using TLS v1.2 with a 4096-bit key (this includes internal transports)	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
34	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt sensor communication – Traffic from the sensors to the platform is always initiated by the sensor and is outbound-only over port 443. Traffic is encrypted via SSL communication using TLS 1.2 with a 4096-bit key.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
35	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support Single sign-on (SSO) authentication methods.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
36	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support Two-Factor Authentication (2FA).	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
37	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should have disaster recovery procedures and redundancies in place to minimize disruption.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
38	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should service strive to provide a 99.95% or better uptime.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
39	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should be able to partition/segregate customer data from other users.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Clause Amended Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
40	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should not access, store, or process any Personally Identifiable Information (PII) or Protected Health Information (PHI).	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
41	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should have all data in all states in the cloud platform is encrypted with at least one level of encryption, using no less than AES-256.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Clause Amended Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
42	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should propose unified modern attack surface visibility.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
43	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support the ability to produce reports in the following report formats: Json, CSV, XML.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should support the ability to produce reports in the following report formats: CSV & PDF.	Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
44	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 :- Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	License to be Provided No .of FQDNs- Minimum 1000 FQDNs	Sizing Queries:- 1. Please provide the Number of location hosting these applications. 2. Data retention policy for Web application scanning data.	1. Please provide the Number of location hosting these applications- On Premise Solution. Console to be deployed at One Location and Unlimited Scanner to be placed as per OCAC's requirement 2. Data retention policy for Web application scanning data.- 180 Days

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
45	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 :- Section :- 21.5.2.4. Project Citation Format	85	Project Citation Format	We request to please confirm if project citation can be provided for Saas/on premise deployment for WAS solution, as funtionality of the solution is similar only model of deployment is as per client requirement.	Project Citation can be provided for SaaS/on premise deployment of WAS Solution
46	4.1 , Pt 6	22	Bidder and OEM should have ISO 9001:2015, ISO 20000:2018, ISO 27001:2013 / ISO 27001:2022 Certifications	Cyble has ISO 27001 and SOC2 certificate which covers all of necessary compliances required in other certificates. For this solution, Request for modification "**bidder and OEM should have ISO 27001 and SOC2 certification**" as this will keep certifications simple and will still include all required compliances	Clause Amended:- Please refer corrigendum.
47	21.5.2.1	59	The OEM solution must comply to the following certifications: A. ISO/IEC 27701:2019 for Privacy Information Management System B. ISO 9001 Compliant	Cyble has ISO 27001 and SOC2 certificate which covers all of necessary compliances required in other certificates. For this solution, Request for modification "**bidder and OEM should have ISO 27001 and SOC2 certification**" as this will keep certifications simple and will still include all required compliances	Clause Amended:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
48	21.5.2.1	62	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	Request you to keep SLA per day for the IOCs as IOCs are updated based on dynamic ratings, and it automatically starts deprecting the score with time. This keeps the score similar whether the scan is done every hour or every day.	As per RFP
49	21.5.2.1	66	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. For image results there should be an option to disable viewing/blurring of images or reporting it.	Will this be required as feed or as cases in the RFP? While we will include the images from the platforms, Cyble doesn't get slow from any image processing, so we can display the images without having any lag.Disabling and Blurring of images is a feature very specific to one OEM, **so we request you to kindly remove it.**	Clause Amended:- Please refer corrigendum
50	21.5.2.1	71	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	Apart from credentials, these malware also steal a lot of files from the infected endpoint. **We request you to also add that files being taken out of the system should also be monitored for OCAC data**	As per RFP
51	21.5.2.1	71	The solution must have option to restrict view of cleartext password for limited admin users only	Restriction in Cyble can be done on the feature itself. Basically, a user can be restricted in accessing the feature or feature upto a certain limit. This allows people without admin acess in a restricted manner. Please suggest if this will be okay for the RFP.	As per RFP. If the Role Based access control suffice the requirement of RFP then it is acceptable

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
52	21.5.2.1	72	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.	**This can be done without a plugin.** Will that suffice the requirement. Plugin is limited for one OEM only, and we therefore we request yout o make it conditional.	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome.
53	21.5.2.1	72	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 IOCs being shown on the page for reducing triage time for analyst.	T**his can be done without a plugin**. Will that suffice the requirement. Plugin is limited for one OEM only, and we therefore we request yout o make it conditional.	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome.
54	21.5.2.1	72	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, Domain, 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 extension 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.	These points are limited to one OEM only. These ate private specs for the same, and we request you to remove them as will it be favorable only that OEM.	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					desired outcome.
55	21.5.2.1	73	The browser extension must have the capability to upload suspicious file URLs for detonation and analysis to OEM offered sandbox solution	This can be done without a plugin. Will that suffice the requirement. Plugin is limited for one OEM only, and we therefore we request yout o make it conditional.	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome.
56	Additional Point to add in the specification	Additional Point	We also suggest that AD integration will be present for the solution, so that OCAC can clearly differentiate between data of current users of OCAC vs old users of OCAC	Additional Point to add in the specification	Bidder have to provide the solution based on present environment.

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
Firm Name:- **Aujas**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**
1	Section 4.1. Eligibility Criteria (Sl. No. 1 Legal Entity, (ii))	20	The bidder office/s must have been in Odisha.	We request for relaxation for this requirement mentioned in Eligibility Criteria. Bidder having national presence in key centres of India would be able to meet RFP requirements.	As per RFP
2	Section 4.1. Eligibility Criteria(Sl. No. 8 Local Office)	22	The bidder should have presence in Odisha with support Centers.	We request for relaxation for this requirement mentioned in Eligibility Criteria. Bidder having national presence in key centres of India would be able to meet RFP requirements.	As per RFP
Firm Name:- **Checkpoint**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**
1	Section 21.5.1.1. Specification for Firewall; Sub Section 1 Hardware Specification; Clause 1.5	54	The appliance should have minimum 4 Ports of 10Gbps SFP+	**Changes Require:** To be deleted **Justification**: Ports requirement are on higher side and are not in line with other performance parameters. Therefore, request to remove the clause.	As per RFP
2	Section 21.5.1.1. Specification for Firewall; Sub Section 1 Hardware Specification; Clause 1.6	54	The appliance should have minimum 1 x Expandable Slots support with optional 8 x SFP/Copper or 4 x SFP+ Port for future requirement	**Changes Require**: To be deleted **Justification**: Ports requirement are on higher side and are not in line with other performance parameters.	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
				Therefore, request to remove the clause.	
3	Section 21.5.1.1. Specification for Firewall; Sub Section 1 Hardware Specification; Clause 1.8	54	The appliance should have minimum internal storage of 1TB SSD for Logs & Reports or better.	**Changes Require**: The management server should have minimum internal storage of 1TB SSD for Logs & Reports or better. **Justification**: Logs needs to be stored in management server and storage require in firewall are for OS and data processing therefore amend the changes as suggested.	It's already mentioned the RFP about that "The appliance should have minimum internal storage of 1TB SSD for Logs & Reports or better."
4	Section 21.5.1.1. Specification for Firewall; Sub Section 1 Hardware Specification; Clause 1.9	54	The appliance Should have Minimum 16GB DDR4 Memory or better	**Changes Require:** The appliance Should have Minimum 64GB DDR4 Memory or better**.** **Justification:** Memory is an integral part of firewall hardware which holds all connections and sessions therefore request to amend the clause as suggested.	As per RFP
4	Section 21.5.1.1. Specification for Firewall; Sub Section 1 Hardware Specification; Clause 1.11	54	The appliance should have Hot Swappable Power Supply	**Changes Require**: The appliance should have Hot Swappable/Redundant Power Supply **Justification**: Each OEM have their own architecture and we ensure continuos running of appliance with dual power supply. Request to amend the clause as suggested.	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
5	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.2	55	The appliance should be able to handle minimum 500K new session per second or better	**Changes Require**: The appliance should be able to handle minimum 300K new session per second or better **Justification**: New Connection per second wrt throughput ask of 10Gbps with NGFW is on higher side and not in line with other performance parameters. Request to amend the clause suggested.	As per RFP
6	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.4	55	The appliance should have minimum Antivirus Throughput of 12 Gbps or better	**Changes Require**: The appliance should have minimum NGTP Throughput of 9 Gbps or better **Justification**: No OEM provide thoughput basis on the antivirus therefore it should be termed as NGTP	Please refer corrigendum
7	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.8	55	The appliance should have minimum 40000 Number of IPSec VPN Peers supported (Site to Site)	**Changes Require**: The appliance should have minimum 5000 Number of IPSec VPN Peers supported (Site to Site) **Justification**: The number of IPSec VPN asks are on higher side and giving an undue advantage to specific OEM. Therefore, request to amend the clause as suggested.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
8	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.9	55	The appliance should have minimum 40000 Number of IPSec VPN Peers supported (Client to Site)	**Changes Require**: The appliance should have minimum 5000 Number of IPSec VPN Peers supported (Client to Site) **Justification**: The number of IPSec VPN asks are on higher side and giving an undue advantage to specific OEM. Therefore, request to amend the clause as suggested.	Please refer corrigendum
9	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.10	55	The appliance should have minimum 10000 Number of SSL VPN Peers supported (Client to Site)	**Changes Require**: The appliance should have minimum 5000 Number of SSL VPN Peers supported (Site to Site) **Justification**: The number of SSL VPN asks are on higher side and giving an undue advantage to specific OEM. Therefore, request to amend the clause as suggested.	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
10	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.11	55	The appliance should have minimum 20M Concurrent Session/Concurrent Connection	**Changes Require**: The appliance should have minimum 16M Concurrent Session/Concurrent Connection **Justification**: The concurrent connections ask are not in line with other performance parameters and are on higher side so request to amend the clause as suggested.	Any traffic session hitting the Data Centre network/server is unpredictable, So higher Concurrent sessions required to scale and accommodate the growing number of devices and users accessing the network in Data Centre. Higher concurrent session/concurrent connection require to process high volume of traffic in the event of DOS/DDOS attacks,

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					security events, and anomalies, which cause surge of concurrent sessions and prevent / hamper connection of data centre Hence, there is a requirement of high concurrent connections in data Centre firewall.
11	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.12	55	The appliance Should support 85+ Web categories for future upgradation of URL filter license	**Recommended change:** Firewall should have more than 110+ predefined Web Categories from Day One. However, firewall should be able to create custom categories for URL filtering for future upgradation. **Justification:** Considering the high level security requirements and other parameters defined in RFP, it is advised to have the highest count of protection against predefined vendor	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
				categories. Hence request to change this clause to harden overall security posture.	
12	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.13	55	The appliance Should support 5000+ application Signature for future upgradation of APP filter license	**Recommended change:** The appliance should have 9000+ predefined application signatures from Day One. However, firewall should have the option to add custom application signatures as well for future upgradation **Justification:** Considering the high level security requirements and other parameters defined in RFP, it is advised to have the highest count of protection against predefined vendor categories. Hence request to change this clause to harden overall security posture.	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
13	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.14	55	The appliance Should support 25000+ IPS Signature for future upgradation of Next generation IPS license	**Changes Require:** The appliance Should support 14000+ IPS Signature for future upgradation of Next generation IPS license. **Justification:** Restrictive clause, request to amend the clause for wider participation.	Higher number of IPS signatures increase the breadth of threat coverage and actively blocking potentially malicious traffic based on signatures. Since asked 25000+ signatures are available with majority of the OEM and there is no requirement of custom IPS signatures. Since OEM tested IPS signatures are more reliable and secure than custom signatures.

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
14	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.16	55	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.	Recommended change: Clause deletion. Justification: Clasue aligned to a specific OEM	As per RFP
15	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.17	55	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	Recommended change: Clause deletion. Justification: Clasue aligned to a specific OEM	As per RFP
16	Section 21.5.1.1. Specification for Firewall; Sub Section Other Terms and Conditions; Clause 5	56	The proposed OEM should Comply with Make in India as per Public Procurement Act (Preference to Make in India)	Make In India Clause. Restricting clause and request to remove the clause for wider participation.	Please refer corrigendum
17	Section 21.5.1.1. Specification for Firewall; Sub Section Other Terms and Conditions; Clause 9	56	The bidder should be ISO certified organization.	Changes Require: The OEM should be in Gartner Leader Quadrant for NGFW category from past 5 yrs.	As per RFP
18	Section 21.5.1.1. Specification for Firewall; Sub Section Other Terms and Conditions; Clause 6	56	The product shall comply minimum 60% and Above Local content or higher.	Make In India Clause. Restricting clause and request to remove the clause for wider participation.	Please refer corrigendum
Firm Name:- **Sify**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
1	4.1. Pre-Qualification (PQ) / Eligibility Criteria	19, 20	1. <u>Legal Entity</u> i. The bidder must be a company registered in India under Indian Companies Act 1956/2013 OR A Partnership firm registered under Indian Partnership Act, 1932. ii. The bidder office/s must have been in Odisha. iii. The bidder must be in operation in India since last 5 years as on 31st December 2023. The bidder must have GST registration & up-to-date Income Tax Return, Valid PAN Number as on 31st March 2023. Note: - In case of no Office in Odisha, self-certification stating that the awarded bidder shall have their office registered in Odisha within 30 days from the award of the contract.	For wider participation we would request OCAC to kindly amend the clause as suggested below: i. The bidder must be a company registered in India under Indian Companies Act 1956/2013 OR A Partnership firm registered under Indian Partnership Act, 1932. ii. The bidder / **Group Company / Parent Company** office/s must have been in Odisha. iii. The bidder must be in operation in India since last **3** years as on 31st December 2023. The bidder must have GST registration & up-to-date Income Tax Return, Valid PAN Number as on 31st March 2023. Note: - In case of no Office in Odisha, self-certification stating that the awarded bidder shall have their office registered in Odisha within 30 days from the award of the contract.	Documentary evidence of the Parent Company for Eligibility Criteria compliance may be submitted

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
2	4.1. Pre-Qualification (PQ) / Eligibility Criteria	20	2. <u>Average Sales Turnover</u> Annual average Turnover during any three financial years out of last five financial year ending March – 2023 (as per the last published Balance sheets), should be as follows: a. Package – I - Minimum of Rs. 10 Crores generated from IT Hardware supply and associated maintenance services. b. Package – II - Minimum of Rs. 30 Crores generated from Supply of Security Software Solution.	For wider participation we would request OCAC to kindly amend the sub-criteria for Package - II as suggested below: b. Package – II - Minimum of Rs. 30 Crores generated from Supply of **IT / ITeS** Solution.	Clause Amended:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
3	4.1. Pre-Qualification (PQ) / Eligibility Criteria	20, 21	5. <u>Technical Capability</u> The Bidder/OEM must have successfully undertaken at least the following numbers of systems implementation engagement(s) of value specified herein during the last three financial years i.e. 2020-21, 2021-22 & 2022-23: . . . . Package – I − One project of similar nature not less than the amount Rs. 1 crore; OR − Two projects of similar nature, each of which not less than the amount Rs. 60 Lakh. − Three projects of similar nature, each of which not less than the amount Rs. 40 Lakhs. − Package – II − One project of similar nature not less than the amount Rs. 3 crores; OR − Two projects of similar nature, each of which not less than the amount Rs. 2 Crores. − Three projects of similar nature, each of which not less than the amount Rs. 1.5 crore. − 'Similar Nature' is defined as, ...	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company incorporated under Companies Act, 2013 as a wholly owned subsidiary of the main Parent Company. In view of the above we would request OCAC to kindly consider the documentary evidence of relevant projects delivered by both the Parent Company and the Subsidiary Company (Bidder) for Eligibility Criteria compliance. Please confirm the acceptance of our request.	Documentary evidence of relevant projects delivered by the Parent Company for Eligibility Criteria compliance may be submitted

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
4	4.1. Pre-Qualification (PQ) / Eligibility Criteria	20, 21	5. <u>Technical Capability</u> 'Similar Nature' is defined as: **Package – I:** "Similar Nature" is defined as: supply, installation & commissioning of Network and Security Components (Enterprise grade Firewall must be the major component within Security Components and should have functionalities asked in the RFP) Government/Semi Government/ PSU/ Scheduled Banks. **Package – II**: "Similar Nature" is defined as: supply, installation & support of Enterprise Security Solution (Threat Intel Platform & Web Scanning Tool should be the major component and should be inclusive of all three solutions) Government/Semi Government/ PSU/ Scheduled Banks.	The definition of "Similar Nature" is restrictive; to promote wider participation we would request OCAC to kindly consider all projects wherein any IT Security Solution has been delivered as 'Similar Nature' for Eligibility Criteria compliance.	As per RFP
5	4.1. Pre-Qualification (PQ) / Eligibility Criteria	22	8. <u>Local Office</u> The bidder should have presence in Odisha with support Centers	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company incorporated under Companies Act, 2013 as a wholly owned subsidiary of the main Parent Company. In view of the above we would request OCAC to kindly consider the office premise of the Parent Company for Eligibility Criteria compliance.	Documentary evidence the Parent Company for Eligibility Criteria compliance may be submitted

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
				Please confirm the acceptance of our request.	
6	4.2.2. Technical Evaluation Criteria for Package – II	24	1. Bidder/OEM should have experience in Threat Intel Solution for SOC environment as per functionalities of Threat Intel Platform Mentioned in RFP - Section 21.5.2.1	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company incorporated under Companies Act, 2013 as a wholly owned subsidiary of the main Parent Company. In view of the above we would request OCAC to kindly consider the documentary evidence of relevant projects delivered by both the Parent Company and the Subsidiary Company (Bidder) for Technical Evaluation Criteria compliance. Further, we would request OCAC to consider similar project experience for scoring. Please confirm the acceptance of our requests.	Documentary evidence of relevant projects delivered by the Parent Company for Eligibility Criteria compliance may be submitted

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
7	4.2.2. Technical Evaluation Criteria for Package – II	24	2. Bidder/OEM should have experience in Threat Integration Platform for SOC environment as per functionalities of Threat Integration Platform Mentioned in RFP - Section 21.5.2.2	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company incorporated under Companies Act, 2013 as a wholly owned subsidiary of the main Parent Company. In view of the above we would request OCAC to kindly consider the documentary evidence of relevant projects delivered by both the Parent Company and the Subsidiary Company (Bidder) for Technical Evaluation Criteria compliance. Further, we would request OCAC to consider similar project experience for scoring. Please confirm the acceptance of our requests.	Documentary evidence of relevant projects delivered by the Parent Company for Eligibility Criteria compliance may be submitted

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
8	4.2.2. Technical Evaluation Criteria for Package – II	24	3. Bidder/OEM should have experience in Supply, Installation and Support of Web Scanning Tool for Data Centre- Section 21.5.2.3	During the FY 2020-21 our organization underwent an internal re-structuring exercise where in the Business Unit relevant for this RFP has been moved to a new company incorporated under Companies Act, 2013 as a wholly owned subsidiary of the main Parent Company. In view of the above we would request OCAC to kindly consider the documentary evidence of relevant projects delivered by both the Parent Company and the Subsidiary Company (Bidder) for Technical Evaluation Criteria compliance. Further, we would request OCAC to consider similar project experience for scoring. Please confirm the acceptance of our requests.	Documentary evidence of relevant projects delivered by the Parent Company for Eligibility Criteria compliance may be submitted
9	8.3.2. SLA for Package - II	33, 34	Penalty	We would request OCAC to kindly cap the upper limit of the penalties to 5% of the PO value.	As per RFP
10	9.1.1. Warranty & Support	39	iv. On-site support from the Bidder.	1. Please confirm if we need to deploy onsite support resources. 2. If response to the above query is 'yes', then please confirm the minimum number of resources and their level [L1 / L2 / L3].	Based on the nature of requirement it's upto Bidder to provide the support.

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
11	9.1.3. Project Deliverables, Milestones & Time Schedule	39	1. Delivery of Equipment - 4 Weeks from date of issue of Purchase Order to the Bidder 2. Installation, Configuration & Integration - 6 Weeks from date of issue of Purchase Order to the Bidder 3. UAT, Sign-off - 8 Weeks from date of issue of Purchase Order to the Bidder 4. Training (Knowledge Transfer) - Within 10 Weeks from date of issue of Purchase Order to the Bidder	In view of the size and complexity of the assignment we would request OCAC to kindly amend the delivery timelines as suggested below: 1. Delivery of Equipment - **8** Weeks from date of issue of Purchase Order to the Bidder 2. Installation, Configuration & Integration - **12** Weeks from date of issue of Purchase Order to the Bidder 3. UAT, Sign-off - **16** Weeks from date of issue of Purchase Order to the Bidder 4. Training (Knowledge Transfer) - Within **20** Weeks from date of issue of Purchase Order to the Bidder	As per RFP
12	10. Details on Scope of Work for Package - II	41	iv) Solution should be easily integrated with existing SIEM solution of CSOC.	Please provide the complete details (solution name, version, release, sizing) of the existing SOC / Security solutions which has to be integrated.	The current SIEM is in the Year Magic Quadrant 2022
13	10. Details on Scope of Work for Package - II	41	viii) Both bidder and OEM will be responsible for the maintenance, configuration and fault free operations of supplied infrastructure i.e. hardware, software and its maintenance during the warranty and post warranty. ix) Any technical glitch/ issue in installed infrastructure of the solution (i.e. hardware and software, OS/DB etc.) should be attended on priority and should be covered under warranty/AMC.	1. Please confirm if we need to deploy onsite support resources. 2. If response to the above query is 'yes', then please confirm the minimum number of resources and their level [L1 / L2 / L3].	Based on the nature of requirement it's upto Bidder to provide the support.

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
14	10.2. Project Deliverables, Milestones & Time Schedule	42	1. Delivery of Tools - 4 Weeks from date of issue of Purchase Order to the Bidder 2. Installation, Configuration & Integration - 8 Weeks from date of issue of Purchase Order to the Bidder 3. Training (Knowledge Transfer) - Within 10 Weeks from date of Purchase Order to the Bidder	In view of the size and complexity of the assignment we would request OCAC to kindly amend the delivery timelines as suggested below: 1. Delivery of Equipment - **8** Weeks from date of issue of Purchase Order to the Bidder 2. Installation, Configuration & Integration - **14** Weeks from date of issue of Purchase Order to the Bidder 3. UAT, Sign-off - **20** Weeks from date of issue of Purchase Order to the Bidder 4. Training (Knowledge Transfer) - Within **24** Weeks from date of issue of Purchase Order to the Bidder	As per RFP
15	20.2. Payment Schedules for Package - I	46	1. Delivery of Equipment & Verification - 60% of the contract value 2. Installation, Configuration, Integration - 30% of the contract value 3. Training (Knowledge Transfer) & UAT - 10% of the contract value	To align with the payment terms of similar assignments we would request OCAC to amend the payment schedule as suggested below: 1. Delivery of Equipment & Verification - 70% of the contract value 2. Installation, Configuration, Integration - 20% of the contract value 3. Training (Knowledge Transfer) & UAT - 10% of the contract value	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
16	20.3. Payment Schedules for Package - II	46	1. Delivery of Solution - 60% of the contract value 2. Installation, Configuration, Integration & UAT - 20% of the contract value 3. Training (Knowledge Transfer) - 10% of the contract value	To align with the payment terms of similar assignments we would request OCAC to amend the payment schedule as suggested below: 1. Delivery of Equipment & Verification - 70% of the contract value 2. Installation, Configuration, Integration - 20% of the contract value 3. Training (Knowledge Transfer) & UAT - 10% of the contract value	As per RFP
17	Section :- 9.1 (iii)	38	The implementation of this project is extremely critical for CSOC wherein the entire demographics of the Network/server infrastructure setup are going to be realigned. Hence the bidder is expected to use the services of OEM nominated professional services who will be present and be involved in the critical tasks from day 1(One). The OEM professional services are supposed to impart the following services but not limited to the same.	Please confirm if OEM's Professional Support (PS) is required to be present physically onsite or remote support would be allowed for providing implementation & support services.	Based on the nature of requirement it's upto Bidder to provide the support.
18	Section :- page no.-42, 10.3	42	1 Threat Intel Solution 01 Solution 2 Threat Integration Platform 01 Solution	Kindly clarify the understanding of "Threat Intel Solution" and "Threat Integration Platform" in context of this particular RFP.	Technical details of Threat Intel Solution and Threat Integration Platform provided in RFP. However Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					may be referred for same
19	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should support (DAST) dynamic application security testing. The proposed solution should provide as SaaS offering that is hosted from within India location data centers.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause asks for SaaS offering, hence request to please change this point as below The proposed solution should support (DAST) dynamic application security testing. The proposed solution should be deployed on premise with unified/single console for existing Infra Vulnerability management & Web application scanning solution part of this RFP.	Please refer corrigendum
20	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose elastic asset licensing.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to SaaS offering. Hence request to remove this clause.	Please refer corrigendum
21	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution must allow users to scan their RESTful API endpoints by providing a Swagger or OpenAPI specification file.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to SaaS offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
22	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose unified Web App Scanning and Vulnerability Management.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an functionality for SaaS offering, hence request to please change this point as below The proposed solution should propose unified console for Web App Scanning procured under this RFP and existing Infra Vulnerability Management Solution.	Please refer corrigendum
23	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should be hosted on the cloud.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an functionality for SaaS offering, hence request to please change this point as below The proposed solution should be deployed on premise.	Please refer corrigendum
24	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should achieve SSAE16 SOC 2 and/or CSA Star certification.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to SaaS offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
25	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose cloud and on-prem scanners.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an functionality for SaaS offering, hence request to please change this point as below The proposed solution should offers on premise scanners.	Please refer corrigendum
26	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose scanners that managed by the platform, e.g. updates to vulnerability signatures, code, and other updates.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an functionality for SaaS offering, hence request to please change this point as below 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.	Please refer corrigendum
27	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt data at rest - data is stored on encrypted media using at least one level of AES-256 encryption.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to SaaS offering. Hence request to remove this clause.	Please refer corrigendum
28	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt data in transit - data is encrypted in transport using TLS v1.2 with a 4096-bit key (this includes internal transports)	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to SaaS offering. Hence request to remove this clause.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
29	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt sensor communication – Traffic from the sensors to the platform is always initiated by the sensor and is outbound-only over port 443. Traffic is encrypted via SSL communication using TLS 1.2 with a 4096-bit key.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to SaaS offering. Hence request to remove this clause.	Please refer corrigendum
30	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support Single sign-on (SSO) authentication methods.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to SaaS offering. Hence request to remove this clause.	Please refer corrigendum
31	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support Two-Factor Authentication (2FA).	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to SaaS offering. Hence request to remove this clause.	Please refer corrigendum
32	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should have disaster recovery procedures and redundancies in place to minimize disruption.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to SaaS offering. Hence request to remove this clause.	Please refer corrigendum
33	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should service strive to provide a 99.95% or better uptime.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to SaaS offering. Hence request to remove this clause.	Please refer corrigendum
34	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should be able to partition/segregate customer data from other users.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
				related to SaaS offering. Hence request to remove this clause.	
35	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should not access, store, or process any Personally Identifiable Information (PII) or Protected Health Information (PHI).	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to SaaS offering. Hence request to remove this clause.	Please refer corrigendum
36	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should have all data in all states in the cloud platform is encrypted with at least one level of encryption, using no less than AES-256.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to SaaS offering. Hence request to remove this clause.	Clause Amended Please refer corrigendum
37	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should propose unified modern attack surface visibility.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to SaaS offering. Hence request to remove this clause.	Please refer corrigendum
38	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support the ability to produce reports in the following report formats: Json, CSV, XML.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an functionality for SaaS offering, hence request to please change this point as below The proposed solution should support the ability to produce reports in the following report formats: CSV & PDF.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
39	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	License to be Provided No .of FQDNs- Minimum 1000 FQDNs	Sizing Queries:- 1. Please provide the Number of location hosting these applications. 2. Data retention policy for Web application scanning data.	1. Please provide the Number of location hosting these applications- On Premise Solution. Console to be deployed at One Location and Unlimited Scanner to be placed as per OCAC's requirement 2. Data retention policy for Web application scanning data.- 180 Days
40	Section :- 21.5.2.4. Project Citation Format	85	Project Citation Format	We request to please confirm if project citation can be provided for SaaS/on premise deployment for WAS solution, as functionality of the solution is similar only model of deployment is as per client requirement.	Project Citation can be provided for SaaS/on premise deployment of WAS Solution

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
Firm Name:- **Bharti Airtel**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**
1	**21.5.2.1. Specification for Threat Intel Solution**	59	Vendor must have Minimum 10 years expertise in anti–malware research/Threat Research	We would request you to consider minimum 7+ years expertise in anti-malware research/Threat research	Clause Amended:- Please refer corrigendum
2		59	Platform should provide the UI in multiple languages(Eg.(i) Arabic (ii) Chinese (both simplified and traditional script) (iv) Farsi (Persian) (v) French (vi) German (vii) Japanese (viii) Russian (ix) Spanish (x) English) & support Summarization & translation of the information	Platform supports scraping the data from multiple languages and from sources across the globe, but the UI itself doesn't have that capability	Clause Amended:- Please refer corrigendum
3		59	The OEM solution must comply to the following certifications: A. ISO/IEC 27701:2019 for Privacy Information Management System B. ISO 9001 Compliant	We would request you to consider ISO 27001 and ISO 9001	Clause Amended:- Please refer corrigendum
4		60	Platform should provide an IOC Lookup feature, where customer will get IOC Risk Score, Confidence Score, Source details, TA profile & IOA	CloudSEK platform currently doesn't have a UI based IOC lookup feature, although IOCs are being provided to the clients	As per RFP
5		62	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	This would be a part of the IOC lookup feature not being currently covered	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
6		66	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.	This would be a part of the IOC Lookup feature not being covered	As per RFP
7		67	Social Media Monitoring: The platform should monitor all the major social media platform, including, but not limited to; Twitter, Facebook, YouTube, Instagram, LinkedIn, Tiktok,Vimeo, RSS All data sources should be collectively analyzed 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. 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.	CloudSEK platform has a rich source inventory where multiple sources for brand related issues including but not limited to social media platforms like Facebook, Twitter, Instagram, LinkedIn, and video sharing websites like YouTube are indexed. Any mentions of the client assets across these sources would be detected and contexualised on the platform. These mentions are then also manually analysed and verified by a team of security researchers and proactive alerts are sent to the client to mitigate these threats TikTok and Vimeo are not being covered as sources yet	Clause Amended:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
8		67	The Bidder/OEM should be member of International Anti-Phishing Working Group (APWG). Solution should provide the visibility of DNS records, Whois records, MX records, screenshot tagged to a typoquatted domain Solution should provide Domain Watclisting feature, to get instant alert whenever there's a change in the status of domain Platform should be capable of doing Image/Logo monitoring to identify profile impersonation Finding domains and emails mentions on Code Repository websites like Github etc CXOs fake social media profiles, posts, pages and groups, takedown is also expected here.	CloudSEK complies with all the requirements ,however Cloudsek isnt a member of APWG. We request you to kindly consider this.	Clause Amended:- Please refer corrigendum
9		70	The solution should show information about spam attacks in which the requested object is attached to email messages.	Feature not being covered, Requesting you to kindly remove the point as it is OEM specific	Clause Deleted Please refer Corrigendum
10		71	The solution must have option to restrict view of cleartext password for limited admin users only	Since CloudSEK already has a feature to create role-based access controls where the accesses themselves can be modularised, we kindly request you to remove this point from the specifications	As per RFP. If the Role Based access control suffice the requirement of RFP then it is acceptable

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
11		71	Clicking links in documents for Microsoft Office (Word, Excel, PowerPoint, Publisher, Outlook) and Adobe Reader	CloudSEK would be able to detect any documents containing mentions of the client's assets, although the links present in those documents would not be scanned for. Requesting to kindly consider this iterations	Clause Deleted:- Please refer corrigendum
12			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 OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
13		72	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 critical, medium and low severity.	Browser extension not being offered, Requesting you to kindly remove the point as it is OEM specific	The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
14			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 IOCs being shown on the page for reducing triage time for analyst.		The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
15			The browser extension must have capability to block potentially malicious links on the webpage being reviewed by the analyst		The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					desired outcome
16			The browser extension must have the option to enable or disable automatic detection of IOCs like IP, Domain, URL, hash and vulnerability (CVE)		The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
17			The browser extension must work with the following solutions Anomaly ThreatStream, ArcSight ESM, ELK (Dashboard only), MISP, Qualys, The Hive Project, VirusTotal etc		The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
18			The browser extension 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 OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the desired outcome
19			The browser extension must have the capability to upload suspicious file URLs for detonation and analysis to OEM offered sandbox solution.		The OEM needs to justify and demonstrate how they can perform the IOC enrichment function on any third party webpage such as SIEM, SOAR, Firewall, IPS, EDR/XDR etc. This may be via browser plugin or any similar way to achieve the

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					desired outcome
20		73	Dynamic Malware Sandboxing should be available: The service should support malware sandboxing by allowing users to a. Upload suspicious files to the platform and download a detailed file behavior analysis report and network analysis report for each uploaded file 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 c. The sandbox should protect organizational privacy by not uploading the file to any publicly accessible repository or third party B. The sandboxing should support operating systems such as Windows, Linux, Mac IoS & Android at a minimum. C. The service should support automated analysis of at-least 50 samples per day D. The service provider should provide analyst support for report interpretation and explanation as and when required.	Sandbox not being offered,Requesting you to kindly remove the point as it is OEM specific	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
21		73	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	MITRE ATT&CK Framework is being followed for report creation	As per RFP
22		73	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		As per RFP
23		74	Incident Response Services (a) On-demand Malware Analysis and Reverse Engineering Assistance (b) On-demand Computer Forensics Analysis, Log Analysis, and Investigation	CloudSEK currently does not provide incident response services, Requesting you to kindly remove the point as it is OEM specific	Clause Deleted Please refer Corrigendum
24	4.1. Pre-Qualification (PQ) / Eligibility Criteria SL. 6 - Quality Certifications	22	Bidder and OEM should have ISO 9001:2015, ISO 20000:2018, ISO 27001:2013 / ISO 27001:2022 Certifications.	Bidder and OEM should have ISO 9001:2015, ISO 20000:2018, ISO 27001:2013 / ISO 27001:2022/SOC2 Certifications.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
25	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should support (DAST) dynamic application security testing. The proposed solution should provide as SaaS offering that is hosted from within India location data centers.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause asks for Saas offering, hence request to please change this point as belowThe proposed solution should support (DAST) dynamic application security testing. The proposed solution should be deployed on premise with unified/single console for existing Infra Vulnerability management & Web application scanning solution part of this RFP.	Please refer Corrigendum
26	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose elastic asset licensing.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
27	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution must allow users to scan their RESTful API endpoints by providing a Swagger or OpenAPI specification file.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
28	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose unified Web App Scanning and Vulnerability Management.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should propose unified console for Web App Scanning	Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
				procured under this RFP and existing Infra Vulnerability Management Solution.	
29	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should be hosted on the cloud.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should be deplyed on premise.	Please refer Corrigendum
30	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should achieve SSAE16 SOC 2 and/or CSA Star certification.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
31	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose cloud and on-prem scanners.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should offers on premise scanners.	Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
32	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	81	The proposed solution should propose scanners that managed by the platform, e.g. updates to vulnerability signatures, code, and other updates.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below 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.	Please refer Corrigendum
33	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt data at rest - data is stored on encrypted media using at least one level of AES-256 encryption.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
34	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt data in transit - data is encrypted in transport using TLS v1.2 with a 4096-bit key (this includes internal transports)	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
35	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	83	The proposed solution should encrypt sensor communication – Traffic from the sensors to the platform is always initiated by the sensor and is outbound-only over port 443. Traffic is encrypted via SSL communication using TLS 1.2 with a 4096-bit key.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
36	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support Single sign-on (SSO) authentication methods.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
37	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support Two-Factor Authentication (2FA).	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
38	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should have disaster recovery procedures and redundancies in place to minimize disruption.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Clause Amended Please refer Corrigendum
39	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should service strive to provide a 99.95% or better uptime.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
40	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should be able to partition/segregate customer data from other users.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
41	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should not access, store, or process any Personally Identifiable Information (PII) or Protected Health Information (PHI).	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
42	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should have all data in all states in the cloud platform is encrypted with at least one level of encryption, using no less than AES-256.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
43	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should propose unified modern attack surface visibility.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is related to Saas offering. Hence request to remove this clause.	Please refer Corrigendum
44	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	The proposed solution should support the ability to produce reports in the following report formats: Json, CSV, XML.	As per RFP we understand the on premise solution is required for Web application scanning, & this clause is an funtionality for Saas offering, hence request to please change this point as below The proposed solution should support the ability to produce reports in the following report formats: CSV & PDF.	Please refer Corrigendum
45	Section :- 21.5.2.3. Specification for Web Application Scanning (WAS) Tool	84	License to be Provided No .of FQDNs- Minimum 1000 FQDNs	Sizing Queries:- 1. Please provide the Number of location hosting these applications. 2. Data retention policy for Web application scanning data.	1. Please provide the Number of location hosting these applications- On Premise Solution. Console to be deployed at One Location and Unlimited Scanner to be

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					placed as per OCAC's requirement 2. Data retention policy for Web application scanning data.- 180 Days
46	Section :- 21.5.2.4. Project Citation Format	85	Project Citation Format	We request to please confirm if project citation can be provided for Saas/on premise deployment for WAS solution, as funtionality of the solution is similar only model of deployment is as per client requirement.	Project Citation can be provided for SaaS/on premise deployment of WAS Solution
47	Section 21.5.1.1. Specification for Firewall; Sub Section 1 Hardware Specification; Clause 1.5	54	The appliance should have minimum 4 Ports of 10Gbps SFP+	**Changes Require:** To be deleted **Justification**: Ports requirement are on higher side and are not in line with other performance parameters. Therefore, request to remove the clause.	As per RFP
48	Section 21.5.1.1. Specification for Firewall; Sub Section 1 Hardware Specification; Clause 1.6	54	The appliance should have minimum 1 x Expandable Slots support with optional 8 x SFP/Copper or 4 x SFP+ Port for future requirement	**Changes Require**: To be deleted **Justification**: Ports requirement are on higher side and are not in line with other performance parameters. Therefore, request to remove the clause.	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
49	Section 21.5.1.1. Specification for Firewall; Sub Section 1 Hardware Specification; Clause 1.8	54	The appliance should have minimum internal storage of 1TB SSD for Logs & Reports or better.	**Changes Require**: The management server should have minimum internal storage of 1TB SSD for Logs & Reports or better. **Justification**: Logs needs to be stored in management server and storage require in firewall are for OS and data processing therefore amend the changes as suggested.	It's already mentioned the RFP about that "The appliance should have minimum internal storage of 1TB SSD for Logs & Reports or better."
50	Section 21.5.1.1. Specification for Firewall; Sub Section 1 Hardware Specification; Clause 1.9	54	The appliance Should have Minimum 16GB DDR4 Memory or better	**Changes Require:** The appliance Should have Minimum 64GB DDR4 Memory or better**.** **Justification:** Memory is an integral part of firewall hardware which holds all connections and sessions therefore request to amend the clause as suggested.	As per RFP
51	Section 21.5.1.1. Specification for Firewall; Sub Section 1 Hardware Specification; Clause 1.11	54	The appliance should have Hot Swappable Power Supply	**Changes Require**: The appliance should have Hot Swappable/Redundant Power Supply **Justification**: Each OEM have their own architecture and we ensure continuos running of appliance with dual power supply. Request to amend the clause as suggested.	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
52	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.2	55	The appliance should be able to handle minimum 500K new session per second or better	**Changes Require**: The appliance should be able to handle minimum 300K new session per second or better **Justification**: New Connection per second wrt throughput ask of 10Gbps with NGFW is on higher side and not in line with other performance parameters. Request to amend the clause suggested.	As per RFP
53	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.4	55	The appliance should have minimum Antivirus Throughput of 12 Gbps or better	**Changes Require**: The appliance should have minimum NGTP Throughput of 9 Gbps or better **Justification**: No OEM provide thoughput basis on the antivirus therefore it should be termed as NGTP	Please refer corrigendum
54	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.8	55	The appliance should have minimum 40000 Number of IPSec VPN Peers supported (Site to Site)	**Changes Require**: The appliance should have minimum 5000 Number of IPSec VPN Peers supported (Site to Site) **Justification**: The number of IPSec VPN asks are on higher side and giving an undue advantage to specific OEM. Therefore, request to amend the clause as suggested.	Please refer corrigendum
55	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.9	55	The appliance should have minimum 40000 Number of IPSec VPN Peers supported (Client to Site)	**Changes Require**: The appliance should have minimum 5000 Number of IPSec VPN Peers supported (Client to Site) **Justification**: The number of IPSec VPN asks are on higher side and giving an undue advantage to specific OEM.	Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
				Therefore, request to amend the clause as suggested.	
56	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.10	55	The appliance should have minimum 10000 Number of SSL VPN Peers supported (Client to Site)	**Changes Require**: The appliance should have minimum 5000 Number of SSL VPN Peers supported (Site to Site) **Justification**: The number of SSL VPN asks are on higher side and giving an undue advantage to specific OEM. Therefore, request to amend the clause as suggested.	As per RFP
57	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.11	55	The appliance should have minimum 20M Concurrent Session/Concurrent Connection	**Changes Require**: The appliance should have minimum 16M Concurrent Session/Concurrent Connection **Justification**: The concurrent connections ask are not in line with other performance parameters and are on higher side so request to amend the clause as suggested.	Any traffic session hitting the Data Centre network/server is unpredictable, So higher Concurrent sessions required to scale and accommodate the growing number of devices and users accessing the network in Data Centre. Higher

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
					concurrent session/concurrent connection require to process high volume of traffic in the event of DOS/DDOS attacks, security events, and anomalies, which cause surge of concurrent sessions and prevent / hamper connection of data centre Hence, there is a requirement of high concurrent connections in data Centre firewall.

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
58	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.12	55	The appliance Should support 85+ Web categories for future upgradation of URL filter license	**Recommended change:** Firewall should have more than 110+ predefined Web Categories from Day One. However, firewall should be able to create custom categories for URL filtering for future upgradation. **Justification:** Considering the high level security requirements and other parameters defined in RFP, it is advised to have the highest count of protection against predefined vendor categories. Hence request to change this clause to harden overall security posture.	As per RFP
59	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.13	55	The appliance Should support 5000+ application Signature for future upgradation of APP filter license	**Recommended change:** The appliance should have 9000+ predefined application signatures from Day One. However, firewall should have the option to add custom application signatures as well for future upgradation **Justification:** Considering the high level security requirements and other parameters defined in RFP, it is advised to have the highest count of protection against predefined vendor categories. Hence request to change this clause to harden overall security posture.	As per RFP

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
60	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.14	55	The appliance Should support 25000+ IPS Signature for future upgradation of Next generation IPS license	**Changes Require:** The appliance Should support 14000+ IPS Signature for future upgradation of Next generation IPS license. **Justification:** Restrictive clause, request to amend the clause for wider participation.	Higher number of IPS signatures increase the breadth of threat coverage and actively blocking potentially malicious traffic based on signatures. Since asked 25000+ signatures are available with majority of the OEM and there is no requirement of custom IPS signatures. Since OEM tested IPS signatures are more reliable and secure than custom signatures.

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
61	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.16	55	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.	Recommended change: Clause deletion. Justification: Clasue aligned to a specific OEM	As per RFP
62	Section 21.5.1.1. Specification for Firewall; Sub Section 3 Performance Capacity Minimum; Clause 3.17	55	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	Recommended change: Clause deletion. Justification: Clasue aligned to a specific OEM	As per RFP
63	Section 21.5.1.1. Specification for Firewall; Sub Section Other Terms and Conditions; Clause 5	56	The proposed OEM should Comply with Make in India as per Public Procurement Act (Preference to Make in India)	Make In India Clause. Restricting clause and request to remove the clause for wider participation.	Please refer corrigendum
64	Section 21.5.1.1. Specification for Firewall; Sub Section Other Terms and Conditions; Clause 9	56	The bidder should be ISO certified organization.	Changes Require: The OEM should be in Gartner Leader Quadrant for NGFW category from past 5 yrs.	As per RFP
65	Section 21.5.1.1. Specification for Firewall; Sub Section Other Terms and Conditions; Clause 6	56	The product shall comply minimum 60% and Above Local content or higher.	Make In India Clause. Restricting clause and request to remove the clause for wider participation.	Please refer corrigendum
Firm Name:- **SCS Tech**					
Sl. No.	**RFP Document Reference & Section**	**Page No**	**Content of RFP requiring clarification**	**Point of Clarification**	**Clarification by OCAC**
1	Section 4 Criteria for Evaluation Clause 4.1 (2b) Average Sales Turnover	20	Package – II - Minimum of Rs. 30 Crores generated from Supply of Security Software Solution.	Request you to please amend the clause as "Package – II - Minimum of Rs. 10 Crores generated from Supply of Security Software Solution." Security Solution	Clause Amended:- Please refer corrigendum

Response to Pre-Bid Queries - OCAC-CERT-CYS-0001-2023-24035 Dtd.28/02/2024					
				Sales is including both hardware and software. Since only software is being considered, request you to reduce the value for increased participation.	
2	Section 4 Criteria for Evaluation Clause 4.1 (5) Technical Capability	21	Package – II – One project of similar nature not less than the amount Rs. 3 crores; OR – Two projects of similar nature, each of which not less than the amount Rs. 2 Crores. – Three projects of similar nature, each of which not less than the amount Rs. 1.5 crore. – 'Similar Nature' is defined as, “Similar Nature” is defined as: supply, installation & support of Enterprise Security Solution (Threat Intel Platform & Web Scanning Tool should be the major component and should be inclusive of all three solutions) Government/Semi Government/ PSU/ Scheduled Banks.	Request you to please modify the clause as Package – II – One project of similar nature not less than the amount Rs. 3 crores; OR – Two projects of similar nature, each of which not less than the amount Rs. 2 Crores. – Three projects of similar nature, each of which not less than the amount Rs. 1.5 crore. – 'Similar Nature' is defined as, “Similar Nature” is defined as: supply, installation & support of Enterprise Security Solution (SIEM including Threat Intel Platform) Government/Semi Government/ PSU/ Scheduled Banks.	As per RFP