Pre Bid Queries for the GeM Bid Ref No GEM/2022/B/2649347 dated 20/10/2022 for providing Anti-Phishing, Anti-Pharming, Anti-Malware, Anti-Trojan, Rogue attacks, Website defacement and Dark Web Monitoring managed services for Period of 3 years.

Sl. No.	GeM Bid Clause	Clause/Technical Specification	Bidder's Query	Bank's Reply
1	Anexure 1-Scope Of Work	1.5. Detect & Stop Email Fraud/Phishing - Actively blocking business email compromises or fraudsters' emails spoofing Bank's domains before they reach Canara Bank employees and customers.	In order to provide protection against Business Email Compromise attacks, an inline email inspection solution is more suitable and will provide high percentage of security. Does Canara Bank looking for having such inline protection? If yes then request Canara Bank to provide below additional information - 1) Which type of Email service is being used - Cloud Email (Gmail/O365) or on-premises? 2) How many number of Email users Canara Bank has?	Bank requires the inteligence / alerts and action, like takedown has to be taken based on the Bank's requirement
2	Anexure 1-Scope Of Work	2.3. Solution must support scanning to a depth of multiple pages	Does Canara Bank expectation to scan their websites? If yes then request to provide the list of all official domains and websites that need to be scanned?	Yes. There are approx 45 domains which will be shared to selected bidder.
3	Anexure 1-Scope Of Work	2.6 Bidder must manage incidents for MMC infection/injecting including solution, coordination for recovery in the shortest possible time.	1) What is the expectation Canara Bank having for management of such detection because the solution only provides alerts and notifications? 2) What is the scope of coordination that Canara Bank is expecting for recovery for such incidents?	Recommendation has to be provided by the bidder for mitigate such execusions.
4	Anexure 1-Scope Of Work	2.16. Solution should not impact the functioning of website. Any configuration done on the Bank's infrastructure for the purpose of monitoring should not impact or degrade the performance of the website.	1) What is the scope of Forensics investigation that Canara Bank is expecting such as - Identification of Threat Actor TTPs, Identification of Threat Actor campaign infrastructure, Identification and evidence gathering of real people behind the targeted campaign, working with Law Enforcement agencies to catch cyber criminals or forensics of Canara Bank Web servers, Email servers and systems to find information related to targeted attacks?	Bidder has to comply with RFP terms and conditions
5	Anexure 1-Scope Of Work	5. Email Fraud Protection: Email fraud is on the rise, business email compromise (BEC) and consumer phishing are at an all-time high. Vendor to Gain visibility into who is sending emails across your enterprise and suggest blocking emails sent from unauthorized sources.	In order to provide protection against Business Email Compormise attacks, an inline email inspection solution is more suitable and will provide high percentage of security. Does Canara Bank looking for having such inline protection? If yes then request Canara Bank to provide below additional information 1) Which type of Email service is being used - Cloud Email (Gmail/O365) or on-premise? 2) How many number of Email users Canara Bank has?	Bank requires the inteligence / alerts and action, like takedown has to be taken based on the Bank's requirement
6	Anexure 1-Scope Of Work	9. Web Site/Web app related Monitoring: 9.6. The successful bidder should identify defacement of Bank website and corresponding Webpages through a combination of automated scans and manual analysis.	Request to provide the list of all Canara Bank Websites?	Approx 45 domains. Detail will be shared with selected bidder.

D.I.T. Wing, Procurement Group
CANARA BANK
H.O., Bengaluru - 560 001

7	Anexure 1-Scope Of Work	14.Followings are the important terms of SLA but not limited to: 14.4. Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident.	Based on the Industry standard response and benchmark for performing global takedowns for last 11 years, we request Canara Bank to change the SLAs as below - 1) Avg guaranteed SLA of 24 hours for Phishing resources in a month 2) Avg guaranteed SLA of 7 days for Scam and trademarks abuses on web & social media platforms in a month.	Kindly refer to Corrigendum-2 for the amended clause
8	Generic EMD AND Epbg	1.EMD Detail Advisory Bank Bank Of Baroda EMD Percentage(%) 1.00 EMD Amount 177000 ePBG Detail Advisory Bank Bank of India ePBG Percentage(%) 3.00 Duration of ePBG required (Months). 38.	1.How the EMD amount of 177000 INR is derived when the EMD percentage is 1%. 2.EMD should be submitted at the time of bidding. I hope my understanding is correct. What should be the mode of EMD (Demand Draft of Bank Guarantee)? 3.ePBG should be submitted which will be 3% of the contract value once the PO is issued. I hope my understanding is correct?	1.EMD amount is arrived as per extant guidelines 2.Bidder can submit EMD in the mode of DD or Bank guarantee 3.Yes.ePBG should be submitted which will be 3% of the total contract value once the PO is issued
9	Anexure 1-Scope Of Work	2.1. Solution must be a tool based automated solution with e-mail and SMS Alerts and integrated with contemporary convergent technologies for gathering intelligence through multi sources and dark web.	We can send SMS alert based on specific alerts manually. As the platform alerts are manually analyzed before the reports are shared, this reduces the false positives to be reviewed by the bank.	Bidder has to comply with RFP terms and conditions
10	Anexure 1-Scope Of Work	3. Early Phishing Detection: 3.9. Monitoring spam traps to detect phishing mails.	What is the bank's expectation in monitoring spam traps? The bidder must be informed about phishing emails received by the bank so corrective measures can be provided by the bidder to the bank.	Bidder has to comply with RFP terms and conditions
11	Anexure 1-Scope Of Work	5. Email Fraud Protection: Email fraud is on the rise, business email compromise (BEC) and consumer phishing are at an all-time high. Vendor to Gain visibility into who is sending emails across your enterprise and suggest blocking emails sent from unauthorized sources.	We would be able to identify public facing emails that are shared on the internet. However; we will ensure that we help in takedown of alerts received by the bank as well	Bank requires the inteligence / alerts and action, like takedown has to be taken based on the Bank's requirement
12	Anexure 1-Scope Of Work	8. Brand Protection and Monitoring: 8.3. Search engines (like Google, yahoo, bing etc.) listing frauds where the customer care number & branch address of banks is changed/ modified should be continuously tracked and the same should be brought down immediately including True caller and JustDial.	Will canara bank provide complete details of customer care number and address for each and every branch location in India? This will help us in monitoring for any change on the internet.	Details will be shared with selected bidder.
13	Anexure 1-Scope Of Work2	9. Web Site/Web app related Monitoring: 9.2. Inject fake credentials into the phishing portals and provide details to bank for monitoring and blocking at Bank's end.	Expectation from bidder? Is the bank expectation is to understand MO of the threat actor? Or is it to understand the phishing exercise. If so, how many times a year?	Yes. As per the requirement of the Bank.

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560 001

14	Anexure 1-Scope Of Work	9. Web Site/Web app related Monitoring: 9.9. The solution should support Authenticated scanning with different authentication methods.	Is the bank expecting the bidder to perform VAPT exercise to the external applications?	Bidder has to comply with RFP terms and conditions
15	Anexure 1-Scope Of Work	9. Web Site/Web app related Monitoring: 9.6. The successful bidder should identify defacement of Bank website and corresponding Webpages through a combination of automated scans and manual analysis.	What are the current change management processes under which the bidder will be informed on minor changes and corrections made by the bank for their websites and its applications to reduce false positives that will not fall under website defacement	Details will be shared with selected bidder.
16	Anexure 1-Scope Of Work	14. Followings aré the important terms of SLA but not limited to: 14.4. Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident.	Usually takes more time than 6 hours to takedown a site	Kindly refer to Corrigendum-2 for the amended clause
17	Anexure 1-Scope Of Work	10. Threat Intelligence Platform: 10.1. Threat Intelligence must be gathered from various sources, ranging from public sources, technical sources, dark web & deep web, Honeypot sensors, Underground forums, special access sites, Code Repositories, Paste bin and human analyst 10.2. Threat intelligence feed should identify new global threats around the globe like Malicious IP Addresses, Domain, URL, Filename, File hash, Email address, Known C&C (Command and Control) hosts, Geolocation feeds like Lat long, AS Number, ISP, Country, etc. 10.3. Collection of Threat intelligence from the various sources should be automated, using technologies such as machine learning and Deep Language Processing, which allows mass collection of intelligence with low false positives, in real-time. 10.4. Threat Intelligence of IOCs must be delivered with full context of related entities, such as related hashes, IPs, CVEs and Threat Actors, Threat Vectors, Malwares, Product impacted etc. The contextualized threat information should be delivered in a simple and easy to digest format. 10.5. Platform should support STIX and TAXII format for integration with SIEM and SOAR.	Bidder request to remove it as this is not really part of Brand Protection or Dark Web monitoring. Threat Intelligence Platform usually gets delivered through SIEM platform under SOC Services	Bidder has to comply with RFP terms and conditions

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560001

18	13. Penalties & Liquidated damages		This should be clarified more, failed to report when we detected - is ok, if other source reports the threat we need to review why/if it could be found via external tools. For example, if client receives a phishing email and we are not monitoring their email gateway then we wouldn't detect it naturally.	Bidder has to comply with RFP terms and conditions
19	13. Penalties & Liquidated damages	13.3. Failure to resolve incidences like Phishing, Pharming, Brand Abuse, Malware etc. (calculated on quarterly average basis for all incidents):	This should be clarified more, failed to report when we detected - is ok, if other source reports the threat we need to review why/if it could be found via external tools. For example, if client receives a phishing email and we are not monitoring their email gateway then we wouldn't detect it naturally.	Bidder has to comply with RFP terms and conditions
20	13. Penalties & Liquidated damages	13.4. Failure to resolve Trojan incidents (To be calculated on incident basis):	Bidder request to remove this clause. These cases are rare (not really clear what type of threats they are relating to - but that's not the point), all these penalties add up to making the service unattainable.	Bidder has to comply with RFP terms and conditions
21	13. Penalties & Liquidated damages	13.6. Failure to maintain response time for Scanning of Bank's websites for Defacement (To be calculated on incident basis):	Should be changed to 30 minutes, as the scan itself takes 30+- to run, and then will begin again. All penalties should be limited to a total amount of no more than 10%	Bidder has to comply with RFP terms and conditions
22	14. Payment terms	14.1. 100% payment shall be released quarterly in arrears after completion of Monitoring services and submission of deliverables (reports and recommendations) and acceptance of the same by the Bank Officials for the respective Assignment.	Request bank to change the terms to 100% yearly in advance	Bidder has to comply with RFP terms and conditions
23	Annexure-2 Technical Evaluation Parameters	No. of years of experience of Bidder in proposed managed services in India.	Requesting you to modify the clause as "No. of years of experience of Bidder/OEM in proposed managed services in India. "	Kindly refer to Corrigendum-2 for the amended clause
24	Annexure-2 Technical Evaluation Parameters	Number of clients for whom the services have been provided by Bidder in India For each client experience -1.5 Marks Maximum marks -15 Marks	Requesting you to modify the clause as "Number of clients for whom the services have been provided by Bidder in India For each client experience -5 Marks Maximum marks -15 Marks "	Bidder has to comply with RFP terms and conditions
25	Annexure-2 Technical Evaluation Parameters	Number of organization in BFSI presently using the proposed services in India. 2-5 customers-10 Marks 6-10 customers-20 Marks >10 customer-25 Marks	Requesting you to modify the clause as "Number of organization in presently using the proposed services in India. 1-3 customers-10 Marks 3-6 customers-20 Marks >6 customer-25 Marks "	Bidder has to comply with RFP terms and conditions
26	Anexure 1-Scope Of Work	2.7.Solution must be independent of application Platform.	Please elaborate it? We're not able to capture what's exactly required here	The solution/service should cover threats for all OS platforms, like Windows, Linux, etc
27	Anexure 1-Scope Of Work	2.3. Solution must support scanning to a depth of multiple pages	How many websites, applications & respective pages are in scope here?	Approx 45 domains. Detail will be shared with selected bidder.
28	Anexure 1-Scope Of Work	2.17. Vendor should assist the Bank in forensic investigation for in scope domains and mobile apps.	How many domains & Mobile apps are in scope here?	Approx 45 domains. Detail will be shared with selected bidder.

I.T. Wing, Procurement Group
CANARA BANK
H.O., Bengaluru-560001

29	Anexure 1-Scope Of Work	7.5. The vendor needs to perform Dark Net/Deep Web forum monitoring for bank registered brand. The vendor should Monitor underground forums, IRC chat rooms, the open web (OSINT) and other communication channels like WhatsApp, Telegram etc where cybercriminals congregate to sell/buy services and tools and exchange knowledge for banks brand	It's not possible to monitor chatters of Cybercrime Channels on Whatsapp, request Bank to remove "Whatsapp".	Kindly refer to Corrigendum-2 for the amended clause
30	Anexure 1-Scope Of Work	14.4. Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident.	Takedown in 6 hours of Incident is very difficult, request bank to increase the time	Kindly refer to Corrigendum-2 for the amended clause
31	Additional Point	Supplier Threat Exposure Reports	We request to add Supplier Threat Exposure module as well, in last couple of years we've observed a lot of Banks impacted due to an exposure at their 3rd Party side, Bank being a significat data fiduciary collects a lot of sensitive personal data from the customers & shares that with the 3rd Parties for further processing of it. It becomes very important to monitor atleast those 3rd Parties who are involved in processing of sensitive data	Bidder has to comply with RFP terms and conditions
32	Additional Point	Sensitive Code Leakage Monitoring	The Platform must monitor cloud repositories, public folders and peer-to-peer networks for data that could represent leaked confidential or sensitive information, enabling Bank to ensure compliance standards and mitigate potential data privacy compliance penalties if any. Code repository must include github, Gitlab & Bitbucket etc.	Bidder has to comply with RFP terms and conditions
33	Additional Point	Misconfigured Cloud Bucket Monitoring		Bidder has to comply with RFP terms and conditions
34	Additional Point	Application SCAN	Banking Web Applications is always on target of the Attackers, we request bank to also include App scan vis a vis OWASP Top 10 Vulnerabilities	Bidder has to comply with RFP terms and conditions
35	Additional Point	Critical Infra Scanning	The Platform must monitor Bank's Infrastructure continuously and provide report on • Exploitable Vulnerabilities from known & Unknown assets • Sensitive Open Port • Certificate Issues • Misconfigured Devices	Bidder has to comply with RFP terms and conditions
36	Additional Point	Integration	Platform should support STIX and TAXII format for integration with SIEM, SOAR & TIP	Bidder has to comply with RFP terms and conditions

D.I.T. Wing, Procurement Group ★ CANARA BANK ★ H.O., Bengaluru-560 001

37	Additional Point	Managed Services	1. **Negotiation as a Service:**In case need to initiate conversation or negotiate with Cyber Criminals in extreme cases with Bank's approval 2. Providing initial analysis of threat intelligence feeds 3. Participation in Security Incident Management Process / Guidelines for severe intelligence findings. 4. Gathering, analysis, and communication of threat intelligence through the intelligence process. 5. Review and analyse external threat intelligence feeds (industry feeds and security partners) 6. Participate in hunting activities based on indicators of compromise or suspicious anomalous activity based on data alerts or data outputs from various toolsets 7.Publish Actionable Intelligence alerts to Bank's SOC analysts for defined use cases (e.g. compromised credentials, Indicators of Compromise associated with active malicious campaigns) 8. Publish Situational Awareness alerts to Bank's SOC team for use cases (e.g. New security threats under consideration that could impact the business) 9. Bi-weekly meeting with Bank's SOC Team 10. Help support, train, guide and coach Bank's SOC Team members on the usage and quality of Threat intelligence feeds. 11. Ad-Hoc on-call off-hours standby support for heightened monitoring initiatives within Bank 12. Report - Monthly Threat Intelligence Report and Management Summary during Monthly, Quarterly, Bi- annual CSOC	Bidder has to comply with RFP terms and conditions
38	Anexure 1-Scope Of Work	1.1. **Visibility** -- Continuous analysis and monitoring of a wide range of sources across emails, web and social media channels with custom and dataset integration like DMARC reports, abuse box and referrer weblogs.	What would be the end goal to achieve the integration with abuse box as abuse box is a email security/email gateway feature?	Bidder has to comply with RFP terms and conditions
39	Anexure 1-Scope Of Work	1.3. **Expedited Attack Takedown** - Rapidly removal of identified threats before customers or employees become aware of a disruption.	Can the client please share the SLA and elaborate the timeline about the expedited attack takedown.	Bidder to refer RFP terms.
40	Anexure 1-Scope Of Work	1.5. **Detect & Stop Email Fraud/Phishing** - Actively blocking business email compromises or fraudsters' emails spoofing Bank's domains before they reach Canara Bank employees and customers.	Actively blocking phishing emails is ideally carried out by Email Security Tool/Firewall. Thus we would request the client to modify the requirement.	Bank requires the inteligence / alerts and action, like takedown has to be taken based on the Bank's requirement

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560001

41	Anexure 1-Scope Of Work	2.6. Bidder must manage incidents for MMC infection/injecting including solution, coordination for recovery in the shortest possible time.	Malicious Mobile Code (MMC) is a term to describe all sorts of destructive programs: viruses, worms, Trojans, and rogue Internet content. These can be prevented by Next-Gen Anti-Virus, Advanced Sandboxing and Using Secure Web Gateways to protect access to the employees. This is beyond the scope of the solution.	Recommendation has to be provided by the bidder for mitigate such execusions.
42	Anexure 1-Scope Of Work	2.7. Solution must be independent of application Platform.	Please elaborate what is implied by "independent of application platform".	The solution/service should cover threats for all OS platforms, like Windows, Linux, etc
43	Anexure 1-Scope Of Work	3.4. Implementation of watermark and other means/techniques for each website.	The proposed methodology is not reliable/effective as Threat Actor Groups can detect and subsequently remove watermarks successfully to run phishing campaigns. The ideal methodology would be to monitor all domains and subdomains which are visually similar for any hosting of websites/logos/watchwords related to the Bank.	Kindly refer to Corrigendum-2 for the amended clause
44	Anexure 1-Scope Of Work	3.5.Implementation of tools for detecting anti - phishing mechanisms such as referrer logs, watermarks etc	The proposed methodology is not reliable/effective as Threat Actor Groups can detect and subsequently remove watermarks successfully to run phishing campaigns. The ideal methodology would be to monitor all domains and subdomains which are visually similar for any hosting of websites/logos/watchwords related to the Bank.	Bidder has to comply with RFP terms and conditions
45	Anexure 1-Scope Of Work	3.6. Track hosting of phishing sites through implementation of watermark and other Means.	The proposed methodology is not reliable/effective as Threat Actor Groups can detect and subsequently remove watermarks successfully to run phishing campaigns. The ideal methodology would be to monitor all domains and subdomains which are visually similar for any hosting of websites/logos/watchwords related to the Bank.	Kindly refer to Corrigendum-2 for the amended clause
46	Anexure 1-Scope Of Work	3.9. Monitoring spam traps to detect phishing mails.	Spam Traps are email addresses that are set up by blacklists, filter companies, and mailbox providers as a way to identify senders with bad list hygiene and list collection practices. This is a capability of email security tool	Bidder has to comply with RFP terms and conditions
47	Anexure 1-Scope Of Work	5. Email Fraud Protection: Email fraud is on the rise, business email compromise (BEC) and consumer phishing are at an all-time high. Vendor to Gain visibility into who is sending emails across your enterprise and suggest blocking emails sent from unauthorized sources.	Best Practice for preventing Business Email Compromise requires two fold approach - Proactive Approach - Via trainning employees on the threat vactors and various mechanisms employed by them for BEC and how to protect themselves from Credential leaks to System compromise. Continuous Monitoring : By the email security tool via setting up advanced sandboxing and detection features to enable timely detection and quarantine. We would request the bank to remove/modify the requirement as it falls under the scope of Employee Security Awareness Trainning and/or Email Security Tool.	Bank requires the inteligence / alerts and action, like takedown has to be taken based on the Bank's requirement
48	Anexure 1-Scope Of Work	6.3. Remove fraudulent mobile applications targeting Bank's customers to capture their credential hosted on popular app stores provided by companies such as Google, Apple and Microsoft etc.	Microsoft as a vendor has stopped making phone softwares.We would like to request the Bank to modify the clause accordingly.	Kindly refer to Corrigendum-2 for the amended clause

Procurement Group
CANARA BANK
Bengaluru-560001

49	Anexure 1-Scope Of Work	7.4. Maintain or have direct access to data from honey pots or network or sensors to collect data on threat.	Can the Bank please elaborate the use case here?	Bidder has to comply with RFP terms and conditions
50	Anexure 1-Scope Of Work	7.5. The vendor needs to perform Dark Net/Deep Web forum monitoring for bank registered brand. The vendor should Monitor underground forums, IRC chat rooms, the open web (OSINT) and other communication channels like WhatsApp, Telegram etc where cybercriminals congregate to sell/buy services and tools and exchange knowledge for banks brand	The proposed solution does support social media monitoring such as Telegram,LinkedIn etc. but Whatsap doesn't provide the access. Thus we would request the Bank to remove Whatsap from the scope.	Kindly refer to Corrigendum-2 for the amended clause
51	Anexure 1-Scope Of Work	8.1. 24x7 anti-phishing services to scan critical websites and Mobile Apps identified by Bank for the tenure of the Contract for Anti-Phishing, Anti-Malware, Anti-Pharming, Anti- Defacement, Anti-Rogue, Anti-Trojan, Dark Web Scanning and any other threat or exploitation of vulnerabilities for unlimited incidents and takedown	We suggest the Bank to indicate a number for Takedowns per year as the costing for Unlimited Takedowns might bear heavily on the overall cost. We suggest a bundle 100 nos Takedowns along with the price of monitoring followed by price for additional takedowns in the multiples of 10 nos as and when needed.	Bidder has to comply with RFP terms and conditions
52	Anexure 1-Scope Of Work	8.4. The service provider is required to perform takedown services (unlimited) subject to identified threat and subsequently bank's approval.	We suggest the Bank to indicate a number for Takedowns per year as the costing for Unlimited Takedowns might bear heavily on the overall cost. We suggest a bundle 100 nos Takedowns along with the price of monitoring followed by price for additional takedowns in the multiples of 10 nos as and when needed.	Bidder has to comply with RFP terms and conditions
53	Anexure 1-Scope Of Work	9.3.Track hosting of phishing sites through implementation of watermark and other means.	The proposed methodology is not reliable/effective as Threat Actor Groups can detect and subsequently remove watermarks successfully to run phishing campaigns. The ideal methodology would be to monitor all domains and subdomains which are visually similar for any hosting of websites/logos/watchwords related to the Bank.	Kindly refer to Corrigendum-2 for the amended clause
54	Anexure 1-Scope Of Work	9.4 Blocking of the phishing sites from search engines and domain registration providers like GoDaddy and others. The bidder needs to have tie ups with search engine providers such as Google, Mozilla, Microsoft and agencies like Cert-In for blocking the phishing sites.	You can not block anybody from buying domain, tie up with search engine providers use different feeds to block or blacklist domains/sites. We would request the bank to modify this clause.	Bidder has to comply with RFP terms and conditions
55	Anexure 1-Scope Of Work	9.9. The solution should support Authenticated scanning with different authentication methods.	Kindly elaborate what is implied by Authenticated Scanning and what different authentication methods are in scope. An example of the use case would help us respond better to the requirement.	Bidder has to comply with RFP terms and conditions

I.T. Wing, Procurement Group
CANARA BANK
H.O., Bengaluru - 560009

56	Anexure 1-Scope Of Work	9.12. The solution should be able to provide website page scanning without skipping (No skipping of page scanning)	This requirement falls under the scope of DAST Tool.	Bidder has to comply with RFP terms and conditions
57	Anexure 1-Scope Of Work	14.2 Alert within 20 minutes of attack/compromise	Please elaborate what constitutes as "attack/compromise". Unlike SIEM and other endpoint tools the proposed solution provides visibility whenever the client is compromised. Details on the scope would help us answer better.	Bidder has to comply with RFP terms and conditions
58	Anexure 1-Scope Of Work	14.3. Initial response to the incident within 20 minutes with action plan on taking down and other alternative response mechanisms.	Please elaborate what constitutes as "incident". Unlike SIEM and other endpoint tools the proposed solution provides visibility whenever the client is compromised. Details on the scope would help us answer better.	Bidder has to comply with RFP terms and conditions
59	Anexure 1-Scope Of Work	14.4. Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident.	Initiation of takedown action within six hours with various hosting engines and social media platforms is possible. However the actual takedown is dependent on the third party, we would request the bank to consider the same and modify the requirement as "Initiate Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident."	Kindly refer to Corrigendum-2 for the amended clause
60	Anexure 1-Scope Of Work	14.7. Phishing site in web on all major browsers such as Internet explorer, Google chrome, Mozilla firefox, Safari, Opera etc. should be blocked within 3 hours of detection of such site	Initiation of takedown action within six hours with various hosting engines and social media platforms is possible. However the actual takedown is dependent on the third party, we would request the bank to consider the same and modify the requirement as "Initiate Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident."	Kindly refer to Corrigendum-2 for the amended clause
61	Anexure 1-Scope Of Work	14.9. Resolution of Trojan incidents with 24 hrs of detection.	Resolution falls under the scope of the Incident Response team of the bank	Bidder has to comply with RFP terms and conditions
62	Anexure 1-Scope Of Work	Bidder has to comply with each point of the above mentioned Scope of Work without any deviations. Non-compliance to any point of the scope of work will lead to disqualification of the Bidder in Technical proposal. Bank may verify the above mentioned points in the Live application provided by the Bidder elsewhere.	Request the Bank to reconsider as there are several points which are addressing "Legacy" forms of attacks or are being achieved by other tools that the Bank has deployed (email security/EDR/NGAV/SIEM) or has approaches which are no longer secure/relevant.	Bidder has to comply with RFP terms and conditions
63	Annexure-2 Technical Evaluation Parameters	No. of years of experience of Bidder in proposed managed services in India.	Request to be modified as - "No. of years of experience of Bidder/OEM in proposed managed services in India."	Kindly refer to Corrigendum-2 for the amended clause
64		Number of clients for whom the services have been provided by Bidder in India	Request to be modified as - "Number of clients for whom the services have been provided by Bidder/OEM in India."	Kindly refer to Corrigendum-2 for the amended clause
65	Pre-Qualification Criteria -Annexure -5	The bidder (including its OEM, if any) should either be Class-I or Class-II local supplier as defined in Public Procurement (Preference to Make in India) Revised Order (English) dated 16/09/2020	Request the Bank to consider an exception to the "Preference to Make in India" clause for this RFP as defined under Government Public Procurement Order No. P-45021/2/2017-PP (BE-II) dated 16.09.2020	Bidder has to comply with RFP terms and conditions
66	Annexure-9	Bill of Material	We suggest the Bank to merge the existing points as a single consolidated price and recommend the bank to modify "unlimited takedowns" as a bundle 100 nos Takedowns along followed by price for additional takedowns in the multiples of 10's as and when needed. This will help in us offering a competitive costing for the Bank.	Bidder has to comply with RFP terms and conditions

Tendering, Procurement Group
CANARA BANK
H.O., Bengaluru-560001

67	Additional Point	Bank to kindly share the list of the Top level Domains, Mobile Apps and Social Media Handles to be monitored.	This will help the bidders to arrive at the costing for the same.	Domains details will be shared with selected bidder.
68	Anexure 1-Scope Of Work	2.7 Solution must be independent of application Platform.	Please elaborate it? We're not able to capture what's exactly required here	The solution/service should cover threats for all OS platforms, like Windows, Linux, etc
69	Anexure 1-Scope Of Work	2.3 Solution must support scanning to a depth of multiple pages	How many websites, applications & respective pages are in scope here?	Approx 45 domains. Detail will be shared with selected bidder.
70	Anexure 1-Scope Of Work	2.17 Vendor should assist the Bank in forensic investigation for in scope domains and mobile apps.	How many domains & Mobile apps are in scope here?	Approx 45 domains. Detail will be shared with selected bidder.
71	Anexure 1-Scope Of Work	7.5 The vendor needs to perform Dark Net/Deep Web forum monitoring for bank registered brand. The vendor should Monitor underground forums, IRC chat rooms, the open web (OSINT) and other communication channels like WhatsApp, Telegram etc where cybercriminals congregate to sell/buy services and tools and exchange knowledge for banks brand	It's not possible to monitor chatters of Cybercrime Channels on Whatsapp, request Bank to remove "Whatsapp".	Kindly refer to Corrigendum-2 for the amended clause
72	Anexure 1-Scope Of Work	14.4 Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident.	Takedown in 6 hours of Incident is very difficult, request bank to increase the time	Kindly refer to Corrigendum-2 for the amended clause
73	Additional Point By vendor	Supplier Threat Exposure Reports	We request to add Supplier Threat Exposure module as well, in last couple of years we've observed a lot of Banks impacted due to an exposure at their 3rd Party side, Bank being a significat data fiduciary collects a lot of sensitive personal data from the customers & shares that with the 3rd Parties for further processing of it. It becomes very important to monitor atleast those 3rd Parties who are involved in processing of sensitive data	Bidder has to comply with RFP terms and conditions
74	Additional Point By vendor	Sensitive Code Leakage Monitoring	The Platform must monitor cloud repositories, public folders and peer-to-peer networks for data that could represent leaked confidential or sensitive information, enabling Bank to ensure compliance standards and mitigate potential data privacy compliance penalties if any. Code repository must include github, Gitlab & Bitbucket etc.	Bidder has to comply with RFP terms and conditions
75	Additional Point By vendor	Misconfigured Cloud Bucket Monitoring		Bidder has to comply with RFP terms and conditions
76	Additional Point By vendor	Application SCAN	Banking Web Applications is always on target of the Attackers, we request bank to also include App scan vis a vis OWASP Top 10 Vulnerabilities	Bidder has to comply with RFP terms and conditions

ng. Procurement Group NARA BANK galuru 560 001

77	Additional Point By vendor	Critical Infra Scanning	The Platform must monitor Bank's Infrastructure continuously and provide report on • Exploitable Vulnerabilities from known & Unknown assets • Sensitive Open Port • Certificate Issues • Misconfigured Devices	Bidder has to comply with RFP terms and conditions
78	Additional Point By vendor	Integration	Platform should support STIX and TAXII format for integration with SIEM, SOAR & TIP	Bidder has to comply with RFP terms and conditions
79	Additional Point By vendor	Managed Services	1. **Negotiation as a Service:**In case need to initiate conversation or negotiate with Cyber Criminals in extreme cases with Bank's approval 2. Providing initial analysis of threat intelligence feeds 3. Participation in Security Incident Management Process / Guidelines for severe intelligence findings. 4. Gathering, analysis, and communication of threat intelligence through the intelligence process. 5. Review and analyse external threat intelligence feeds (industry feeds and security partners) 6. Participate in hunting activities based on indicators of compromise or suspicious anomalous activity based on data alerts or data outputs from various toolsets 7.Publish Actionable Intelligence alerts to Bank's SOC analysts for defined use cases (e.g. compromised credentials, Indicators of Compromise associated with active malicious campaigns) 8. Publish Situational Awareness alerts to Bank's SOC team for use cases (e.g. New security threats under consideration that could impact the business) 9. Bi-weekly meeting with Bank's SOC Team 10. Help support, train, guide and coach Bank's SOC Team members on the usage and quality of Threat intelligence feeds. 11. Ad-Hoc on-call off-hours standby support for heightened monitoring initiatives within Bank 12. Report - Monthly Threat Intelligence Report and Management Summary during Monthly, Quarterly, Bi- annual CSOC	Bidder has to comply with RFP terms and conditions
80	Anexure 1-Scope Of Work	1.1. **Visibility** -- Continuous analysis and monitoring of a wide range of sources across emails, web and social media channels with custom and dataset integration like DMARC reports, abuse box and referrer weblogs.	What would be the end goal to achieve the integration with abuse box as abuse box is a email security/email gateway feature?	Bidder has to comply with RFP terms and conditions
81	Anexure 1-Scope Of Work	1.3. **Expedited Attack Takedown** - Rapidly removal of identified threats before customers or employees become aware of a disruption.	Can the client please share the SLA and elaborate the timeline about the expedited attack takedown.	Bidder has to comply with RFP terms and conditions

I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru - 560001

82	Anexure 1-Scope Of Work	1.5 Detect & Stop Email Fraud/Phishing - Actively blocking business email compromises or fraudsters' emails spoofing Bank's domains before they reach Canara Bank employees and customers.	Actively blocking phishing emails is ideally carried out by Email Security Tool/Firewall. Thus we would request the client to modify the requirement.	Bank requires the inteligence / alerts and action, like takedown has to be taken based on the Bank's requirement
83	Anexure 1-Scope Of Work	2.6 Bidder must manage incidents for MMC infection/injecting including solution, coordination for recovery in the shortest possible time.	Malicious Mobile Code (MMC) is a term to describe all sorts of destructive programs: viruses, worms, Trojans, and rogue Internet content. These can be prevented by Next-Gen Anti-Virus, Advanced Sandboxing and Using Secure Web Gateways to protect access to the employees. This is beyond the scope of the solution.	Recommendation has to be provided by the bidder for mitigate such execusions.
84	Anexure 1-Scope Of Work	2.7 Solution must be independent of application Platform.	Please elaborate what is implied by "independent of application platform".	The solution/service should cover threats for all OS platforms, like Windows, Linux, etc
85	Anexure 1-Scope Of Work	3.4 Implementation of watermark and other means/techniques for each website.	The proposed methodology is not reliable/effective as Threat Actor Groups can detect and subsequently remove watermarks successfully to run phishing campaigns. The ideal methodology would be to monitor all domains and subdomains which are visually similar for any hosting of websites/logos/watchwords related to the Bank.	Kindly refer to Corrigendum-2 for the amended clause
86	Anexure 1-Scope Of Work	3.5. Implementation of tools for detecting anti - phishing mechanisms such as referrer logs, watermarks etc.	The proposed methodology is not reliable/effective as Threat Actor Groups can detect and subsequently remove watermarks successfully to run phishing campaigns. The ideal methodology would be to monitor all domains and subdomains which are visually similar for any hosting of websites/logos/watchwords related to the Bank.	Bidder has to comply with RFP terms and conditions
87	Anexure 1-Scope Of Work	3.6 Track hosting of phishing sites through implementation of watermark and other Means.	The proposed methodology is not reliable/effective as Threat Actor Groups can detect and subsequently remove watermarks successfully to run phishing campaigns. The ideal methodology would be to monitor all domains and subdomains which are visually similar for any hosting of websites/logos/watchwords related to the Bank.	Kindly refer to Corrigendum-2 for the amended clause
88	Anexure 1-Scope Of Work	3.9 Monitoring spam traps to detect phishing mails.	Spam Traps are email addresses that are set up by blacklists, filter companies, and mailbox providers as a way to identify senders with bad list hygiene and list collection practices. This is a capability of email security tool.	Bidder has to comply with RFP terms and conditions

I.T. Wing, Procurement Group
CANARA BANK
H.O., Bengaluru 560 001

89	Anexure 1-Scope Of Work	**5. Email Fraud Protection:** Email fraud is on the rise, business email compromise (BEC) and consumer phishing are at an all-time high. Vendor to Gain visibility into who is sending emails across your enterprise and suggest blocking emails sent from unauthorized sources.	Best Practice for preventing Business Email Compromise requires two fold approach - Proactive Approach - Via trainning employees on the threat vactors and various mechanisms employed by them for BEC and how to protect themselves from Credential leaks to System compromise. Continuous Monitoring : By the email security tool via setting up advanced sandboxing and detection features to enable timely detection and quarantine. We would request the bank to remove/modify the requirement as it falls under the scope of Employee Security Awareness Trainning and/or Email Security Tool.	Bank requires the inteligence / alerts and action, like takedown has to be taken based on the Bank's requirement
90	Anexure 1-Scope Of Work	6.3 Remove fraudulent mobile applications targeting Bank's customers to capture their credential hosted on popular app stores provided by companies such as Google, Apple and Microsoft etc.	Microsoft as a vendor has stopped making phone softwares.We would like to request the Bank to modify the clause accordingly.	Kindly refer to Corrigendum-2 for the amended clause
91	Anexure 1-Scope Of Work	7.4 Maintain or have direct access to data from honey pots or network or sensors to collect data on threat.	Can the Bank please elaborate the use case here?	Bidder has to comply with RFP terms and conditions
92	Anexure 1-Scope Of Work	7.5 The vendor needs to perform Dark Net/Deep Web forum monitoring for bank registered brand. The vendor should Monitor underground forums, IRC chat rooms, the open web (OSINT) and other communication channels like WhatsApp, Telegram etc where cybercriminals congregate to sell/buy services and tools and exchange knowledge for banks brand	The proposed solution does support social media monitoring such as Telegram,LinkedIn etc. but Whatsap doesn't provide the access. Thus we would request the Bank to remove Whatsap from the scope.	Kindly refer to Corrigendum-2 for the amended clause
93	Anexure 1-Scope Of Work	8.1 24x7 anti-phishing services to scan critical websites and Mobile Apps identified by Bank for the tenure of the Contract for Anti-Phishing, Anti-Malware, Anti-Pharming, Anti- Defacement, Anti-Rogue, Anti-Trojan, Dark Web Scanning and any other threat or exploitation of vulnerabilities for unlimited incidents and takedown.	We suggest the Bank to indicate a number for Takedowns per year as the costing for Unlimited Takedowns might bear heavily on the overall cost. We suggest a bundle 100 nos Takedowns along with the price of monitoring followed by price for additional takedowns in the multiples of 10 nos as and when needed.	Bidder has to comply with RFP terms and conditions

Wing, Procurement Group CANARA BANK Bengaluru - 560001

94	Anexure.1-Scope Of Work	8.4. The service provider is required to perform takedown services (unlimited) subject to identified threat and subsequently bank's approval.	We suggest the Bank to indicate a number for Takedowns per year as the costing for Unlimited Takedowns might bear heavily on the overall cost. We suggest a bundle 100 nos Takedowns along with the price of monitoring followed by price for additional takedowns in the multiples of 10 nos as and when needed.	Bidder has to comply with RFP terms and conditions
95	Anexure 1-Scope Of Work	9.3 Track hosting of phishing sites through implementation of watermark and other means.	The proposed methodology is not reliable/effective as Threat Actor Groups can detect and subsequently remove watermarks successfully to run phishing campaigns. The ideal methodology would be to monitor all domains and subdomains which are visually similar for any hosting of websites/logos/watchwords related to the Bank.	Kindly refer to Corrigendum-2 for the amended clause
96	Anexure 1-Scope Of Work	9.4 Blocking of the phishing sites from search engines and domain registration providers like GoDaddy and others. The bidder needs to have tie ups with search engine providers such as Google, Mozilla, Microsoft and agencies like Cert-In for blocking the phishing sites.	You can not block anybody from buying domain, tie up with search engine providers use different feeds to block or blacklist domains/sites. We would request the bank to modify this clause.	Bidder has to comply with RFP terms and conditions
97	Anexure 1-Scope Of Work	9.9 The solution should support Authenticated scanning with different authentication methods.	Kindly elaborate what is implied by Authenticated Scanning and what different authentication methods are in scope. An example of the use case would help us respond better to the requirement.	Bidder has to comply with RFP terms and conditions
98	Anexure 1-Scope Of Work	9.12 The solution should be able to provide website page scanning without skipping (No skipping of page scanning)	This requirement falls under the scope of DAST Tool.	Bidder has to comply with RFP terms and conditions
99	Anexure 1-Scope Of Work	14.2 Alert within 20 minutes of attack/compromise	Please elaborate what constitutes as "attack/compromise". Unlike SIEM and other endpoint tools the proposed solution provides visibility whenever the client is compromised. Details on the scope would help us answer better.	Bidder has to comply with RFP terms and conditions
100	Anexure 1-Scope Of Work	14.3 Initial response to the incident within 20 minutes with action plan on taking down and other alternative response mechanisms.	Please elaborate what constitutes as "incident". Unlike SIEM and other endpoint tools the proposed solution provides visibility whenever the client is compromised. Details on the scope would help us answer better.	Bidder has to comply with RFP terms and conditions
101	Anexure 1-Scope Of Work	14.4 Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident	Initiation of takedown action within six hours with various hosting engines and social media platforms is possible. However the actual takedown is dependent on the third party, we would request the bank to consider the same and modify the requirement as "Initiate Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident."	Kindly refer to Corrigendum-2 for the amended clause
102	Anexure 1-Scope Of Work	14.7 Phishing site in web on all major browsers such as Internet explorer, Google chrome, Mozilla firefox, Safari, Opera etc. should be blocked within 3 hours of detection of such site.	Initiation of takedown action within six hours with various hosting engines and social media platforms is possible. However the actual takedown is dependent on the third party, we would request the bank to consider the same and modify the requirement as "Initiate Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident."	Kindly refer to Corrigendum-2 for the amended clause
103	Anexure 1-Scope Of Work	14.9 Resolution of Trojan incidents with 24 hrs of detection.	Resolution falls under the scope of the Incident Response team of the bank	Bidder has to comply with RFP terms and conditions

104	Anexure 1-Scope Of Work	Bidder has to comply with each point of the above mentioned Scope of Work without any deviations. Non-compliance to any point of the scope of work will lead to disqualification of the Bidder in Technical proposal. Bank may verify the above mentioned points in the Live application provided by the Bidder elsewhere.	Request the Bank to reconsider as there are several points which are addressing "Legacy" forms of attacks or are being achieved by other tools that the Bank has deployed (email security/EDR/NGAV/SIEM) or has approaches which are no longer secure/relevant.	Bidder has to comply with RFP terms and conditions
105	Annexure 2 Technical Evaluation Parameter	No. of years of experience of Bidder in proposed managed services in India.	Request to be modified as - "No. of years of experience of **Bidder/OEM** in proposed managed services in India."	Kindly refer to Corrigendum-2 for the amended clause
106	Annexure 2 Technical Evaluation Parameter	Number of clients for whom the services have been provided by Bidder in India	Request to be modified as - "Number of clients for whom the services have been provided by **Bidder/OEM** in India."	Kindly refer to Corrigendum-2 for the amended clause
107	Annexure-5.Prequalification Criteria	The bidder (including its OEM, if any) should either be Class-I or Class-II local supplier as defined in Public Procurement (Preference to Make in India) Revised Order (English) dated 16/09/2020	Request the Bank to consider an exception to the "Preference to Make in India" clause for this RFP as defined under Government Public Procurement Order No. P-45021/2/2017-PP (BE-II) dated 16.09.2020	Bidder has to comply with RFP terms and conditions
108	Annexure-9.Bill Of material	24x7x365 monitoring of websites and mobile applications for Anti- Phishing, Anti-Pharming & Anti-Trojan, Rogue Attacks, Anti-Malware and Defacement including unlimited takedowns and other services as per Scope of Work & Dark Web Monitoring of websites and mobile applications.	We suggest the Bank to merge the existing points as a single consolidated price and recommend the bank to modify "unlimited takedowns" as a bundle 100 nos Takedowns along followed by price for additional takedowns in the multiples of 10's as and when needed. This will help in us offering a competitive costing for the Bank.	Bidder has to comply with RFP terms and conditions
109	Additional Points by vendor	Bank to kindly share the list of the Top level Domains, Mobile Apps and Social Media Handles to be monitored.	This will help the bidders to arrive at the costing for the same.	Domains details will be shared with selected bidder.
110	Anexure 1-Scope Of Work	1.1. **Visibility** -- Continuous analysis and monitoring of a wide range of sources across emails, web and social media channels with custom and dataset integration like DMARC reports, abuse box and referrer weblogs.	What would be the end goal to achieve the integration with abuse box as abuse box is a email security/email gateway feature?	Bidder has to comply with RFP terms and conditions
111	Anexure 1-Scope Of Work	1.3. **Expedited Attack Takedown** - Rapidly removal of identified threats before customers or employees become aware of a disruption.	Can the client please share the SLA and elaborate the timeline about the expedited attack takedown.	Bidder has to comply with RFP terms and conditions
112	Anexure 1-Scope Of Work	1.5 Detect & Stop Email Fraud/Phishing - Actively blocking business email compromises or fraudsters' emails spoofing Bank's domains before they reach Canara Bank employees and customers.	Actively blocking phishing emails is ideally carried out by Email Security Tool/Firewall. Thus we would request the client to modify the requirement.	Bank requires the inteligence / alerts and action, like takedown has to be taken based on the Bank's requirement

Wing. Procurement Group
CANARA BANK
Bengaluru - 560 001

113	Anexure 1-Scope Of Work	2.6 Bidder must manage incidents for MMC infection/injecting including solution, coordination for recovery in the shortest possible time.	Malicious Mobile Code (MMC) is a term to describe all sorts of destructive programs: viruses, worms, Trojans, and rogue Internet content. These can be prevented by Next-Gen Anti-Virus, Advanced Sandboxing and Using Secure Web Gateways to protect access to the employees. This is beyond the scope of the solution.	Recommendation has to be provided by the bidder for mitigate such execusions.
114	Anexure 1-Scope Of Work	2.7 Solution must be independent of application Platform.	Please elaborate what is implied by "independent of application platform".	The solution/service should cover threats for all OS platforms, like Windows, Linux, etc
115	Anexure 1-Scope Of Work	3.4 Implementation of watermark and other means/techniques for each website.	The proposed methodology is not reliable/effective as Threat Actor Groups can detect and subsequently remove watermarks successfully to run phishing campaigns. The ideal methodology would be to monitor all domains and subdomains which are visually similar for any hosting of websites/logos/watchwords related to the Bank.	Kindly refer to Corrigendum-2 for the amended clause
116	Anexure 1-Scope Of Work	3.5. Implementation of tools for detecting anti - phishing mechanisms such as referrer logs, watermarks etc.	The proposed methodology is not reliable/effective as Threat Actor Groups can detect and subsequently remove watermarks successfully to run phishing campaigns. The ideal methodology would be to monitor all domains and subdomains which are visually similar for any hosting of websites/logos/watchwords related to the Bank.	Bidder has to comply with RFP terms and conditions
117	Anexure 1-Scope Of Work	3.6 Track hosting of phishing sites through implementation of watermark and other Means.	The proposed methodology is not reliable/effective as Threat Actor Groups can detect and subsequently remove watermarks successfully to run phishing campaigns. The ideal methodology would be to monitor all domains and subdomains which are visually similar for any hosting of websites/logos/watchwords related to the Bank.	Kindly refer to Corrigendum-2 for the amended clause
118	Anexure 1-Scope Of Work	3.9 Monitoring spam traps to detect phishing mails.	Spam Traps are email addresses that are set up by blacklists, filter companies, and mailbox providers as a way to identify senders with bad list hygiene and list collection practices. This is a capability of email security tool.	Bidder has to comply with RFP terms and conditions
119	Anexure 1-Scope Of Work	**5. Email Fraud Protection:** Email fraud is on the rise, business email compromise (BEC) and consumer phishing are at an all-time high. Vendor to Gain visibility into who is sending emails across your enterprise and suggest blocking emails sent from unauthorized sources.	Best Practice for preventing Business Email Compromise requires two fold approach - Proactive Approach - Via trainning employees on the threat vactors and various mechanisms employed by them for BEC and how to protect themselves from Credential leaks to System compromise. Continuous Monitoring : By the email security tool via setting up advanced sandboxing and detection features to enable timely detection and quarantine. We would request the bank to remove/modify the requirement as it falls under the scope of Employee Security Awareness Trainning and/or Email Security Tool.	Bank requires the inteligence / alerts and action, like takedown has to be taken based on the Bank's requirement

Wing, Procurement Group
CANARA BANK
H.O, Bengaluru 560002

120	Anexure 1-Scope Of Work	6.3 Remove fraudulent mobile applications targeting Bank's customers to capture their credential hosted on popular app stores provided by companies such as Google, Apple and Microsoft etc.	Microsoft as a vendor has stopped making phone softwares.We would like to request the Bank to modify the clause accordingly.	Kindly refer to Corrigendum-2 for the amended clause
121	Anexure 1-Scope Of Work	7.4 Maintain or have direct access to data from honey pots or network or sensors to collect data on threat.	Can the Bank please elaborate the use case here?	Bidder has to comply with RFP terms and conditions
122	Anexure 1-Scope Of Work	7.5 The vendor needs to perform Dark Net/Deep Web forum monitoring for bank registered brand. The vendor should Monitor underground forums, IRC chat rooms, the open web (OSINT) and other communication channels like WhatsApp, Telegram etc where cybercriminals congregate to sell/buy services and tools and exchange knowledge for banks brand	The proposed solution does support social media monitoring such as Telegram,LinkedIn etc. but Whatsap doesn't provide the access. Thus we would request the Bank to remove Whatsap from the scope.	Kindly refer to Corrigendum-2 for the amended clause
123	Anexure 1-Scope Of Work	8.1 24x7 anti-phishing services to scan critical websites and Mobile Apps identified by Bank for the tenure of the Contract for Anti-Phishing, Anti-Malware, Anti-Pharming, Anti- Defacement, Anti-Rogue, Anti-Trojan, Dark Web Scanning and any other threat or exploitation of vulnerabilities for unlimited incidents and takedown.	We suggest the Bank to indicate a number for Takedowns per year as the costing for Unlimited Takedowns might bear heavily on the overall cost. We suggest a bundle 100 nos Takedowns along with the price of monitoring followed by price for additional takedowns in the multiples of 10 nos as and when needed.	Bidder has to comply with RFP terms and conditions
124	Anexure 1-Scope Of Work	8.4. The service provider is required to perform takedown services (unlimited) subject to identified threat and subsequently bank's approval.	We suggest the Bank to indicate a number for Takedowns per year as the costing for Unlimited Takedowns might bear heavily on the overall cost. We suggest a bundle 100 nos Takedowns along with the price of monitoring followed by price for additional takedowns in the multiples of 10 nos as and when needed.	Bidder has to comply with RFP terms and conditions
125	Anexure 1-Scope Of Work	9.3 Track hosting of phishing sites through implementation of watermark and other means.	The proposed methodology is not reliable/effective as Threat Actor Groups can detect and subsequently remove watermarks successfully to run phishing campaigns. The ideal methodology would be to monitor all domains and subdomains which are visually similar for any hosting of websites/logos/watchwords related to the Bank.	Kindly refer to Corrigendum-2 for the amended clause
126	Anexure 1-Scope Of Work	9.4 Blocking of the phishing sites from search engines and domain registration providers like GoDaddy and others. The bidder needs to have tie ups with search engine providers such as Google, Mozilla, Microsoft and agencies like Cert-In for blocking the phishing sites.	You can not block anybody from buying domain, tie up with search engine providers use different feeds to block or blacklist domains/sites. We would request the bank to modify this clause.	Bidder has to comply with RFP terms and conditions

127	Anexure 1-Scope Of Work	9.9 The solution should support Authenticated scanning with different authentication methods.	Kindly elaborate what is implied by Authenticated Scanning and what different authentication methods are in scope. An example of the use case would help us respond better to the requirement.	Bidder has to comply with RFP terms and conditions
128	Anexure 1-Scope Of Work	9.12 The solution should be able to provide website page scanning without skipping (No skipping of page scanning)	This requirement falls under the scope of DAST Tool.	Bidder has to comply with RFP terms and conditions
129	Anexure 1-Scope Of Work	14.2 Alert within 20 minutes of attack/compromise	Please elaborate what constitutes as "attack/compromise". Unlike SIEM and other endpoint tools the proposed solution provides visibility whenever the client is compromised. Details on the scope would help us answer better.	Bidder has to comply with RFP terms and conditions
130	Anexure 1-Scope Of Work	14.3 Initial response to the incident within 20 minutes with action plan on taking down and other alternative response mechanisms.	Please elaborate what constitutes as "incident". Unlike SIEM and other endpoint tools the proposed solution provides visibility whenever the client is compromised. Details on the scope would help us answer better.	Bidder has to comply with RFP terms and conditions
131	Anexure 1-Scope Of Work	14.4 Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident	Initiation of takedown action within six hours with various hosting engines and social media platforms is possible. However the actual takedown is dependent on the third party, we would request the bank to consider the same and modify the requirement as "**Initiate** Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident."	Kindly refer to Corrigendum-2 for the amended clause
132	Anexure 1-Scope Of Work	14.7 Phishing site in web on all major browsers such as Internet explorer, Google chrome, Mozilla firefox, Safari, Opera etc. should be blocked within 3 hours of detection of such site.	Initiation of takedown action within six hours with various hosting engines and social media platforms is possible. However the actual takedown is dependent on the third party, we would request the bank to consider the same and modify the requirement as "**Initiate** Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident."	Kindly refer to Corrigendum-2 for the amended clause
133	Anexure 1-Scope Of Work	14.9 Resolution of Trojan incidents with 24 hrs of detection.	Resolution falls under the scope of the Incident Response team of the bank	Bidder has to comply with RFP terms and conditions
134	Anexure 1-Scope Of Work	Bidder has to comply with each point of the above mentioned Scope of Work without any deviations. Non-compliance to any point of the scope of work will lead to disqualification of the Bidder in Technical proposal. Bank may verify the above mentioned points in the Live application provided by the Bidder elsewhere.	Request the Bank to reconsider as there are several points which are addressing "Legacy" forms of attacks or are being achieved by other tools that the Bank has deployed (email security/EDR/NGAV/SIEM) or has approaches which are no longer secure/relevant.	Bidder has to comply with RFP terms and conditions
135	Annexure 2 Technical Evaluation Parameter	No. of years of experience of Bidder in proposed managed services in India.	As these services provided from OEM directly and bidder will be used as mode of transaction , Request to be modified as - "No. of years of experience of **Bidder/OEM** in proposed managed services in India."	Kindly refer to Corrigendum-2 for the amended clause
136	Annexure 2 Technical Evaluation Parameter	Number of clients for whom the services have been provided by Bidder in India	As these services provided from OEM directly and bidder will be used as mode of transaction , Request to be modified as - "Number of clients for whom the services have been provided by **Bidder/OEM** in India."	Kindly refer to Corrigendum-2 for the amended clause
137	Annexure-5.Prequalification Criteria	The bidder (including its OEM, if any) should either be Class-I or Class-II local supplier as defined in Public Procurement (Preference to Make in India) Revised Order (English) dated 16/09/2020	Request the Bank to consider an exception to the "Preference to Make in India" clause for this RFP as defined under Government Public Procurement Order No. P-45021/2/2017-PP (BE-II) dated 16.09.2020	Bidder has to comply with RFP terms and conditions

Procurement Group
CANARA BANK
H.O., Bengaluru-560001

138	Annexure-9.Bill Of material	24x7x365 monitoring of websites and mobile applications for Anti- Phishing, Anti-Pharming & Anti-Trojan, Rogue Attacks, Anti-Malware and Defacement including unlimited takedowns and other services as per Scope of Work & Dark Web Monitoring of websites and mobile applications.	We suggest the Bank to merge the existing points as a single consolidated price and recommend the bank to modify "unlimited takedowns" as a bundle 100 nos Takedowns along followed by price for additional takedowns in the multiples of 10's as and when needed. This will help in us offering a competitive costing for the Bank.	Bidder has to comply with RFP terms and conditions
139	Annexure 2 Technical Evaluation Parameter	The number of CISA/CISSP/CEH Certified personnel employed by bidder.	Request bank to amend the clause as "The number of CISA/CISSP/CEH Certified personnel employed by **OEM/Bidder**."	Kindly refer to Corrigendum-2 for the amended clause
140	Annexure 2 Technical Evaluation Parameter	The Bidder/OEM has ISO 27001 Certified Security Operations Centre.	Request bank to amend the clause as "The Bidder/OEM has **ISO 27001 Certified organization**".	Bidder has to comply with RFP terms and conditions
141	Additional Points by vendor	Bank to kindly share the list of the Top level Domains, Mobile Apps and Social Media Handles to be monitored.	This will help the bidders to arrive at the costing for the same.	Approx 45 domains. Detail will be shared with selected bidder.
142	Anexure 1-Scope Of Work	1.5 **Detect & Stop Email Fraud/Phishing** - Actively blocking business email compromises or fraudsters' emails spoofing Bank's domains before they reach Canara Bank employees and customers.	In order to provide protection against Business Email Compormise attacks, an inline email inspection solution is more suitable and will provide high percentage of security. Does Canara Bank looking for having such inline protection? If yes then request Canara Bank to provide below additional information - 1) Which type of Email service is being used - Cloud Email (Gmail/O365) or on-premise? 2) How many number of Email users Canara Bank has?	Bank requires the inteligence / alerts and action, like takedown has to be taken based on the Bank's requirement
143	Anexure 1-Scope Of Work	2.3 Solution must support scanning to a depth of multiple pages	Does Canara Bank expectation to scan their websites? If yes then request to provide the list of all official domains and websites that need to be scanned?	Yes. There are approx 45 domains which will be shared to selected bidder.
144	Anexure 1-Scope Of Work	2.6 Bidder must manage incidents for MMC infection/injecting including solution, coordination for recovery in the shortest possible time.	1) What is the expectation Canara Bank has for management of such detection because the solution only provides alerts and notifications? 2) What is the scope of coordination that Canara Bank is expecting for recovery for such incidents?	Recommendation has to be provided by the bidder for mitigate such execusions.
145	Anexure 1-Scope Of Work	2.16. Solution should not impact the functioning of website. Any configuration done on the Bank's infrastructure for the purpose of monitoring should not impact or degrade the performance of the website	1) What is the scope of Forensics investigation that Canara Bank is expecting such as - Identification of Threat Actor TTPs, Identification of Threat Actor campaign infrastructure, Identification and evidence gathering of real people behind the targeted campaign, working with Law Enforcement agencies to catch cyber criminals or forensics of Canara Bank Web servers, Email servers and systems to find information related to targeted attacks?	Bidder has to comply with RFP terms and conditions

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560001

146	Anexure 1-Scope Of Work	**5. Email Fraud Protection:** Email fraud is on the rise, business email compromise (BEC) and consumer phishing are at an all-time high. Vendor to Gain visibility into who is sending emails across your enterprise and suggest blocking emails sent from unauthorized sources.	In order to provide protection against Business Email Compormise attacks, an inline email inspection solution is more suitable and will provide high percentage of security. Does Canara Bank looking for having such inline protection? If yes then request Canara Bank to provide below additional information - 1) Which type of Email service is being used - Cloud Email (Gmail/O365) or on-premise? 2) How many number of Email users Canara Bank has?	Bank requires the inteligence / alerts and action, like takedown has to be taken based on the Bank's requirement
147	Anexure 1-Scope Of Work	9.6 The successful bidder should identify defacement of Bank website and corresponding Webpages through a combination of automated scans and manual analysis	Request to provide the list of all Canara Bank Websites?	Approx 45 domains. Detail will be shared with selected bidder.
148	Anexure 1-Scope Of Work	14.4 Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident.	Based on the Industry standard response and benchmark for performing global takedowns for last 11 years, we request Canara Bank to change the SLAs as below - 1) Avg guaranteed SLA of 24 hours for Phishing resources in a month 2) Avg guaranteed SLA of 7 days for Scam and trademarks abuses on web & socialmedia platforms in a month.	Kindly refer to Corrigendum-2 for the amended clause
149	3.About RFP:	Scope of Work as per Annexure-1 for providing Anti-Phishing, Anti-Pharming, Anti-Malware, Anti-Trojan, Rogue attacks, Website defacement and Dark Web Monitoring managed services for Period of 3 years.	Kindly share the baseline details for the proposed services - Top Level Domains / URLs, Mobile Apps and Social Media Handles that needs to be monitored.	Domains details will be shared with selected bidder.
150	3.About RFP:	Scope of Work as per Annexure-1 for providing Anti-Phishing, Anti-Pharming, Anti-Malware, Anti-Trojan, Rogue attacks, Website defacement and Dark Web Monitoring managed services for Period of 3 years.	Kindly share the SLAs to be achieved by the bidder for each of the the proposed services.	Bidder to refer RFP terms.
151	10.Delivery	10.2.1. Subscription for Anti-Phishing, Anti-Pharming, Anti-Malware, Anti-Trojan, Rogue attacks, Website defacement and Dark Web Monitoring managed services should be started within **2 weeks** from the date of acceptance of the Purchase Order.	Requesting the Bank to consider a timeframe of 4 weeks from the date of acceptance of the purchase order for starting the subscriptions.	Bidder has to comply with RFP terms and conditions
152	13. Penalties & Liquidated damages	13.2 Penalties/Liquidated damages for each Incident happened and not reported:	Requesting the Bank to kindly provide more clarity on this. If an incident is reported on any un-monitored source, how will the Bank act on it?	Bidder has to comply with RFP terms and conditions

...ing, Procurement Group
CANARA BANK
★ H.O. Bengaluru-560001 ★

153	13. Penalties & Liquidated damages	13.3 Failure to resolve incidences like Phishing, Pharming, Brand Abuse, Malware etc. (calculated on quarterly average basis for all incidents):	Requesting the Bank to consider increasing the 'Resolution Time' for resolving the reported incidents.	Bidder has to comply with RFP terms and conditions
154	13. Penalties & Liquidated damages	13.4 Failure to resolve Trojan incidents (To be calculated on incident basis):	Requesting the Bank to consider increasing the 'Resolution Time' for resolving the Trojan incidents.	Bidder has to comply with RFP terms and conditions
155	13. Penalties & Liquidated damages	13.5 Delay in Takedown of phishing sites and fraudulent mobile apps specifically targeting Canara Bank (Standalone attacks)	Requesting the Bank to consider increasing the 'Resolution Time' for the takedown of phishing sites and fraudulent mobile apps.	Bidder has to comply with RFP terms and conditions
156	13. Penalties & Liquidated damages	13.6 Failure to maintain response time for Scanning of Bank's websites for Defacement (To be calculated on incident basis):	Requesting the Bank to increase the detection time to a mininum of 40 minutes, as the scanning may itself take close to 30 +/- minutes.	Bidder has to comply with RFP terms and conditions
157	13. Penalties & Liquidated damages		Requesting the Bank to consider lowering the penalties limited to a total amount of no more than 10%	Bidder has to comply with RFP terms and conditions
158	31. **Right to Alter Quantities/Location:**	In the event of changes in plans of the Bank, Bank reserves the right to alter the quantities / locations for implementing the services by adding/deleting/substituting the devices/locations, etc., from the one specified in the tender at the same rate arrived on the same terms and conditions of this RFP.	Requesting the Bank to provide more clarity on this.	If any changes during issuance of Purchase Order Bank reserves the right to alter the quantities / locations for implementing the services by adding/deleting/substituting the devices/locations, etc., from the one specified in the tender at the same rate arrived on the same terms and conditions of this RFP
159	33 **Project Execution**	The entire project needs to be completed expeditiously. The Bank and the selected bidder shall nominate a Project Manager each immediately on acceptance of the order, who shall be the single point of contact for the project at Bengaluru. However, for escalation purpose, details of other persons shall also be given. The project manager nominated by the bidder should have prior experience in implementing similar project. Project Kick-Off meeting should happen within 7 days from the date of acceptance of purchase order. The bidder shall submit a Weekly progress report to the Bank as per format, which will be made available to the selected bidder.	Requesting the Bank to consider increasing the timeframe for the Kick-Off meeting to 3 weeks from the date of acceptance of the purchase order.	Bidder has to comply with RFP terms and conditions

Procurement Group CANARA BANK Bengaluru-560 001

160	34 <u>Execution of Agreement</u>	34.1 Within 21 days from the date of acceptance of the Purchase Order or within 30 days from the date of issue of Purchase Order whichever is earlier, the selected bidder shall sign a stamped "Agreement" with the Bank at Bengaluru as per the format provided by the Bank. Failure to execute the Agreement makes the EMD liable for forfeiture at the discretion of the Bank and also rejection of the selected bidder.	Requesting the Bank to consider increasing the timeframe to 45 days from the date of issue of the purchase order for signing the Agreement.	Bidder has to comply with RFP terms and conditions
161	40. Responsibility for Completeness	40.3 The selected bidder shall be responsible for any discrepancies, errors and omissions or other information submitted by him irrespective of whether these have been approved, reviewed or otherwise accepted by the bank or not. The selected bidder shall take all corrective measures arising out of discrepancies, error and omission other information as mentioned above within the time schedule and without extra cost to the bank.	Kindly provide more clarity on the user level demo mentioned here please.	The selected bidder shall be responsible for any discrepancies, errors and omissions or other information submitted by him irrespective of whether these have been approved, reviewed or otherwise accepted by the bank or not. The selected bidder shall take all corrective measures arising out of discrepancies, error and omission other information as mentioned above within the time schedule and without extra cost to the bank. The clause clealy spelt banks requirement on subject condition
162	61.Procurement through Local Suppliers (Make in India):	Department of Industrial Policy and Promotion under Ministry of Commerce and Industry vide letter no. P-45021/2/2017-PP (BE-II) dated 16.09.2020 has notified revised guidelines to be followed to promote manufacturing and production of goods and services in India under "Make in India" initiative.	Request the Bank to consider an exception to the "Preference to Make in India" clause for this RFP as defined under Government Public Procurement Order No. P-45021/2/2017-PP (BE-II) dated 16.09.2020	Bidder has to comply with RFP terms and conditions

I.T. Wing, Procurement Group
CANARA BANK
H.O., Bengaluru-560001

163	61.12 Ministry of Electronics and Information Technology (MeitY):	61.12.1 In furtherance of the Public Procurement (Preference to Make in India) Order 2017 notified vide reference cited above, Ministry of Electronics and Information Technology, Government of India has issued revised Public Procurement (Preference to Make in India) Order 2019 for cyber security products vide reference File No.1(10)/2017-CLES dated 06/12/2019.	Also, in a complex engagement of this type, we would need to collaborate with multiple OEMs to provide the requested services. Hence requesting the Bank to kindly provide an exception to this clause.	Bidder has to comply with RFP terms and conditions
164	Anexure 1-Scope Of Work	1.1. **Visibility** -- Continuous analysis and monitoring of a wide range of sources across emails, web and social media channels with custom and dataset integration like DMARC reports, abuse box and referrer weblogs.	Kindly elaborate on the integration with abuse box, as abuse box is a email security / email gateway feature.	Bidder has to comply with RFP terms and conditions
165	Anexure 1-Scope Of Work	1.5 **Detect & Stop Email Fraud/Phishing** - Actively blocking business email compromises or fraudsters' emails spoofing Bank's domains before they reach Canara Bank employees and customers.	Requesting the Bank to kindly elaborate on this feature, as blocking emails are ideally carried out by Email Security tool / Firewall.	Bank requires the inteligence / alerts and action, like takedown has to be taken based on the Bank's requirement
166	Anexure 1-Scope Of Work	2.7 Solution must be independent of application Platform.	Requesting the Bank to provide more clarity on 'independent of application platform'.	The solution/service should cover threats for all OS platforms, like Windows, Linux, etc
167	Anexure 1-Scope Of Work	**5. Email Fraud Protection:** Email fraud is on the rise, business email compromise (BEC) and consumer phishing are at an all-time high. Vendor to Gain visibility into who is sending emails across your enterprise and suggest blocking emails sent from unauthorized sources.	Requesting the Bank to kindly amend this requirement as this falls under the scope of Employee Security Awareness Trainning and/or Email Security Tool.	Bank requires the inteligence / alerts and action, like takedown has to be taken based on the Bank's requirement
168	Anexure 1-Scope Of Work	6.4 Inject fake credentials into the phishing portals and fraudulent apps and provide details to the Bank for monitoring and blocking at Bank's end.	Need more clarity on this.	Bidder has to comply with RFP terms and conditions
169	Anexure 1-Scope Of Work	7.4. Maintain or have direct access to data from honey pots or network or sensors to collect data on threat.	Requesting the Bank to provide more clarity on this use case please.	Bidder has to comply with RFP terms and conditions

D.I.T. Wing, Procurement Group
CANARA BANK
H.O., Bengaluru 560

170	Anexure 1-Scope Of Work	8.1 24x7 anti-phishing services to scan critical websites and Mobile Apps identified by Bank for the tenure of the Contract for Anti-Phishing, Anti-Malware, Anti-Pharming, Anti- Defacement, Anti-Rogue, Anti-Trojan, Dark Web Scanning and any other threat or exploitation of vulnerabilities for unlimited incidents and takedown. 8.4. The service provider is required to perform takedown services (unlimited) subject to identified threat and subsequently bank's approval.	We suggest the Bank to indicate a number for Takedowns per year as the costing for Unlimited Takedowns might bear heavily on the overall cost. We suggest a bundle 100 Takedowns along with the price of monitoring followed by price for additional takedowns in the multiples of 10 as and when needed.	Bidder has to comply with RFP terms and conditions
171	Anexure 1-Scope Of Work	9.9 The solution should support Authenticated scanning with different authentication methods.	Kindly elaborate what is implied by Authenticated Scanning and what different authentication methods are in scope. An example of the use case would help us respond better to the requirement.	Bidder has to comply with RFP terms and conditions
172	Anexure 1-Scope Of Work	14.4 Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident.	Initiation of takedown action within 6 hours with various hosting engines and social media platforms is possible. However the actual takedown is dependent on the third party,hence we request the Bank to consider the same and modify the requirement as "Initiate Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident."	Kindly refer to Corrigendum-2 for the amended clause
173	Anexure 1-Scope Of Work	14.7 Phishing site in web on all major browsers such as Internet explorer, Google chrome, Mozilla firefox, Safari, Opera etc. should be blocked within 3 hours of detection of such site.	Initiation of blocking the detected site within 3 hours with various hosting engines and social media platforms is possible. However the blocking is dependent on the respective browsers, hence we request the Bank to consider the same and modify the requirement as "Initiate blocking of the Phishing site in web on all major browsers such as Internet explorer, Google chrome, Mozilla firefox, Safari, Opera etc. within 3 hours of detection of such site and block the site as soon as possible."	Kindly refer to Corrigendum-2 for the amended clause
174	Anexure 1-Scope Of Work	14.9 Resolution of Trojan incidents with 24 hrs of detection.	Need more clarity on this. What kind of resolution is expected from the bidder.	Bidder has to comply with RFP terms and conditions
175	Annexure 2 Technical Evaluation Parameter	No. of years of experience of Bidder in proposed managed services in India.	Request to be modified as - "No. of years of experience of Bidder/OEM in proposed managed services in India."	Kindly refer to Corrigendum-2 for the amended clause
176	Annexure 2 Technical Evaluation Parameter	Number of clients for whom the services have been provided by Bidder in India.	Request to be modified as - "Number of clients for whom the services have been provided by Bidder/OEM in India."	Kindly refer to Corrigendum-2 for the amended clause
177	Anexure 1-Scope Of Work	2.3 Solution must support scanning to a depth of multiple pages	How many websites, applications & respective pages are in scope here?	Approx 45 domains. Detail will be shared with selected bidder.
178	Anexure 1-Scope Of Work	2.7 Solution must be independent of application Platform.	Please elaborate it? We're not able to capture what's exactly required here	The solution/service should cover threats for all OS platforms, like Windows, Linux, etc.

D.I.T. Wing, Procurement Group
CANARA BANK
H.O. Bengaluru-560001

179	Anexure 1-Scope Of Work	2.17 Vendor should assist the Bank in forensic investigation for in scope domains and mobile apps.	How many domains & Mobile apps are in scope here?	Approx 45 domains. Detail will be shared with selected bidder.
180	Anexure 1-Scope Of Work	7.5 The vendor needs to perform Dark Net/Deep Web forum monitoring for bank registered brand. The vendor should Monitor underground forums, IRC chat rooms, the open web (OSINT) and other communication channels like WhatsApp, Telegram etc where cybercriminals congregate to sell/buy services and tools and exchange knowledge for banks brand	It's not possible to monitor chatters of Cybercrime Channels on Whatsapp, request Bank to remove "Whatsapp".	Kindly refer to Corrigendum-2 for the amended clause
181	Anexure 1-Scope Of Work	14.4 Take down of Phishing Site, fraudulent mobile apps within 6 hours of incident.	Takedown in 6 hours of Incident is very difficult, request bank to increase the time	Kindly refer to Corrigendum-2 for the amended clause
182	Additional Point	Supplier Threat Exposure Reports	We request to add Supplier Threat Exposure module as well, in last couple of years we've observed a lot of Banks impacted due to an exposure at their 3rd Party side, Bank being a significat data fiduciary collects a lot of sensitive personal data from the customers & shares that with the 3rd Parties for further processing of it. It becomes very important to monitor atleast those 3rd Parties who are involved in processing of sensitive data	Bidder has to comply with RFP terms and conditions
183	ASM	Sensitive Code Leakage Monitoring Misconfigured Cloud Bucket Monitoring	The Platform must monitor cloud repositories, public folders and peer-to-peer networks for data that could represent leaked confidential or sensitive information, enabling Bank to ensure compliance standards and mitigate potential data privacy compliance penalties if any. Code repository must include github, Gitlab & Bitbucket etc.	Bidder has to comply with RFP terms and conditions
185	ASM	Application SCAN	Banking Web Applications is always on target of the Attackers, we request bank to also include App scan vis a vis OWASP Top 10 Vulnerabilities	Bidder has to comply with RFP terms and conditions
186	ASM	Critical Infra Scanning	The Platform must monitor Bank's Infrastructure continuously and provide report on • Exploitable Vulnerabilities from known & Unknown assets • Sensitive Open Port • Certificate Issues • Misconfigured Devices	Bidder has to comply with RFP terms and conditions
187	ASM	Integration	Platform should support STIX and TAXII format for integration with SIEM, SOAR & TIP	Bidder has to comply with RFP terms and conditions

D.S.C. Wing, Procurement Group
CANARA BANK
H.O., Bengaluru-560001

188	Additional Point	Managed Services	1. **Negotiation as a Service:**In case need to initiate conversation or negotiate with Cyber Criminals in extreme cases with Bank's approval 2. Providing initial analysis of threat intelligence feeds 3. Participation in Security Incident Management Process / Guidelines for severe intelligence findings. 4. Gathering, analysis, and communication of threat intelligence through the intelligence process. 5. Review and analyse external threat intelligence feeds (industry feeds and security partners) 6. Participate in hunting activities based on indicators of compromise or suspicious anomalous activity based on data alerts or data outputs from various toolsets 7.Publish Actionable Intelligence alerts to Bank's SOC analysts for defined use cases (e.g. compromised credentials, Indicators of Compromise associated with active malicious campaigns) 8. Publish Situational Awareness alerts to Bank's SOC team for use cases (e.g. New security threats under consideration that could impact the business) 9. Bi-weekly meeting with Bank's SOC Team 10. Help support, train, guide and coach Bank's SOC Team members on the usage and quality of Threat intelligence feeds. 11. Ad-Hoc on-call off-hours standby support for heightened monitoring initiatives within Bank 12. Report - Monthly Threat Intelligence Report and Management Summary during Monthly, Quarterly, Bi- annual CSOC	Bidder has to comply with RFP terms and conditions

Date:09/11/2022
Place:Bangalore.

Deputy General Manager