

Information Technology Division, HO, 5, Sansad Marg, New Delhi – 110 001

Email: itdhw@pnb.co.in

CORRIGENDUM 1

RFP for procurement of Network Anti-Advanced Persistent Threat (N/w- APT) and Deception/Decoy Solution

Sr. No.	Page No.	RFP Clause Name & No.	Existing RFP Clause	Amended Clause
1	46	Technical Specification APT Solution Point 19	The solution should provide summary for instance, whether the malware wrote into a certain file, modified a registry setting, opened a port or communicated to a specific URL, or changed the name of a running process to hide itself.	The solution should provide summary for instance, whether the malware wrote into a certain file, modified a registry setting, opened a port or communicated to a specific URL, or changed the name of a running process to hide itself. This should be done if it is integrated with the existing endpoint APT.
2	35	ELIGIBILITY CRITERIA OF THE BIDDER , ANNEXURE-III, Point 4	The proposed Network Anti-APT solution and Deception/Decoy Solution must have been implemented during the last 3 years as on date of RFP and currently running successfully, in atleast 1 PSU Banks/ Private Banks in India. <i>(One reference each for both the solutions is required)</i>	The proposed Network Anti-APT solution and Deception/Decoy Solution must have been implemented during the last 3 years as on date of RFP and currently running successfully, in atleast 1 PSU Banks/ Private Banks/BFSI/Telecom sector/PSU in India or in any Global Bank having Presence in India <i>(One reference each for both the solutions is required)</i>
3	35	ELIGIBILITY CRITERIA OF THE BIDDER , ANNEXURE-III, Point 5	The bidder must have successfully implemented Anti-APT/ Deception/ Decoy/ Honeypot Solution during the last 3 years as on date of RFP in atleast 1 PSU Banks/ Private Banks/PSU/BFSI in India, which should be currently running successfully.	The bidder must have successfully implemented Anti-APT/ Deception/ Decoy/ Honeypot Solution during the last 3 years as on date of RFP and currently running successfully in atleast 1 PSU Banks/ Private Banks/ PSU/ BFSI/Telecom sector in India or in any Global Bank having

Sr. No.	Page No.	RFP Clause Name & No.	Existing RFP Clause	Amended Clause
				having Presence in India
4	35	Annexure III - ELIGIBILITY CRITERIA OF THE BIDDER - Point No. 6	The bidder and OEM should have Support center in Delhi/NCR and Mumbai.	The bidder should have Support center in Delhi/NCR and Mumbai and the OEM should have support center in India.
5	53	Technical specification of the Offered solution ANNEXURE-XII, Deception Solution, Point 13	The solution should have the ability to capture commands executed for hi-interaction SSH connections on Linux decoys without any instrumentation processes or agents running within the decoys.	The solution should have the ability to capture commands executed for hi-interaction SSH connections on Linux decoys with or without any instrumentation processes or agents running within the decoys.
6	53	Technical specification of the Offered solution ANNEXURE-XII, Deception Solution, Point 19	The solution should have the ability to record the screen in a video (NOT screenshots) and must also capture keystrokes and mouse movements for hi-interaction remote desktop connections on Windows decoys and provide a downloadable video replay with keystroke capture of the attacker's activity in the decoy	The solution should have the ability to capture keystrokes and mouse movements for hi-interaction remote desktop connections on Windows decoys.
7	54	Technical specification of Deception Solution, Point 28	Besides email alerts, the solution must have the built in ability for realtime voice phone calls and SMS alerts based on preset or custom notification rules	Besides email alerts, the solution must have the built-in ability or through third party integration, for real-time voice phone calls and SMS alerts based on preset or custom notification rules
8	54	Annexure XII - Deception Solution - Point No. 37	Solution should provide deep visibility into the Vlans in the form of assests, services, os, etc. and must record and alert incase of any new endpoint connects to the vlan.	Solution should provide deep visibility into any lateral movement in Vlans in the form of services, os, etc. and must record and alert incase of any new endpoint scans/connects to the vlan.
9	55	Annexure XII - Deception Solution - Point No. 43	Solution should automatically detect scanning and L2 attacks such as ARP flood and IP scan etc.	Solution should automatically detect scanning like IP scan etc.
10	55	Annexure XII - Deception Solution - Point No. 44	The solution should support deceptive objects (breadcrumbs) on production endpoints centrally from the management console without relying on 3rd party tools	The solution should support deceptive objects (breadcrumbs) on production endpoints centrally from the management console with or without relying on 3rd party tools
11	55	Annexure XII - Deception Solution - Point No. 51	The solution should integrate with existing patch management solution of the bank to keep the decoys in sync with the patch level of devices in production environment	The solution should keep the decoys in sync with the devices in production environment
12	55	Annexure XII - Deception Solution - Point No. 59	Solution should provide ability to forward emails to sandboxing functionality for email/malware analysis	Solution should provide ability to integrate with 3 rd party tools/sandboxing for malware analysis

Sr. No.	Page No.	RFP Clause Name & No.	Existing RFP Clause	Amended Clause
13	56	Annexure XII - Deception Solution - Point No. 69	The solution should support sending Darknet IP traffic to the platform. Should be able to create unused IP"s in production subnets and dark networks on routers and forward traffic to these IP"s to deceptive VM"s for engagement.	Clause stands deleted
14	56	Annexure XII - Deception Solution - Point No. 70	Solution should be able to spin up or create an automatic decoy as per the request seen from the attacker.	Solution should have the capability, if feasible, to spin up or create an automatic decoy as per the request seen from the attacker.
15	56	Annexure XII - Deception Solution - Point No. 71	System should be able to detect and track stolen credentials by integrating with SIEM on API's	System should be able to detect and track stolen credentials by integrating with SIEM or Active Directory
16	8	Scope of Work Network Anti-APT, Clause No. 3.5	The Solution should be sized for 100Mbps performance throughput and the solution (with each of its components) should be configured in High Availability (HA) mode both at DC&DR. The bidder should size for adequate hardware and related software and the proposed solution should have the functionality to scale both horizontally and vertically.	The Solution should be sized for 4 Gbps performance throughput and the solution (with each of its components) should be configured in High Availability (HA) mode both at DC&DR. The bidder should size for adequate hardware and related software and the proposed solution should have the functionality to scale both horizontally and vertically.
17	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 2	d. Be able to offload sandbox services to the appliance	Be able to do sandbox services within the appliance/ integrated sandbox solution
18	45	Technical Specifications Network Anti-APT, Clause No. 5	The solution should be able to identify malware present in network file shares and web objects (For Eg:JPEG, doc, docx, exe, gif, hip, htm, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx. etc. and any new formats having vulnerabilities to carry potential malware) and able to quarantine them.	The solution should be able to identify malware present in network file shares and web objects (For Eg:JPEG, doc, docx, exe, gif, pdf, png, ppsx, ppt, pptx, rtf, swf, , url, vcf, xls, xlsx. etc. and any new formats having vulnerabilities to carry potential malware) and able to quarantine/block them.
19	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 12	Solution should perform dynamic analysis of files outside of Bank's network, in a space where malware files cannot evade detection. Specifically, malware files should be processed in a dedicated dirty space, with full Internet access that allows bare metal analysis of the malware, to counter VM and Internet aware malware as well as implement other	Solution should perform dynamic analysis of files outside of Bank's network, in a space where malware files cannot evade detection.

Sr. No.	Page No.	RFP Clause Name & No.	Existing RFP Clause	Amended Clause
			controls (such as time dilation, key stroke counts, varying software configuration, etc.)	
20	46	Technical Specifications Network Anti-APT, Clause No. 15	Solution should detect whether malware downloaded by an endpoint was effectively installed (executed) on the endpoint, this done via methodologies that do not utilize endpoint agents i.e. Agentless approach	If it is integrated with endpoint APT, the solution should detect whether malware downloaded by an endpoint was effectively installed (executed) on the endpoint, this should be done via methodologies that do not utilize endpoint agents i.e. Agentless approach.
21	35	Annexure III - ELIGIBILITY CRITERIA OF THE BIDDER - Point No. 2	Bidder and OEM must be an ISO 27001: 2013 or higher certified company.	Bidder/OEM must be an ISO 27001: 2013 or higher certified company.
22	46	Technical Specifications Network Anti-APT, Clause No. 20	The solution should quickly inspect and should discover malicious code at both the CPU and the operating system levels. Discovered malicious files should be prevented from entering the network	The solution should quickly inspect and should discover malicious code at CPU/ operating system levels. Discovered malicious files should be prevented from entering the network
23	46	Technical Specifications Network Anti-APT, Clause No. 21	The solution must have the ability to scrub active content from documents type file providing the user documents with zero active content and deliver a safe copy of the file to the user	Clause Stands deleted
24	46	Technical Specifications Network Anti-APT, Clause No. 23	The Anti-APT solution should support multiple deployment options, providing a cost-effective solution. Files can be sent from existing gateways to an on premise appliance. As part of the already Installed security gateway, the solution should be applied across the entire organization, or implemented only for specific individuals, domains, or departments	Clause Stands deleted
25	47	Technical Specifications Network Anti-APT, Clause No. 26	The solution should have visibility of downloads of malicious mobile applications, infected mobile devices, outdated mobile OS versions, access to high risk web applications and websites, usage of cloud base mobile apps	Clause Stands deleted
26	47	Technical Specifications Network Anti-APT, Clause No.	Solution should be deployed on premise and along with on premise sandboxing capability where the objectionable content may be	Solution should be deployed on premise and along with on premise sandboxing capability where the objectionable content may be

Sr. No.	Page No.	RFP Clause Name & No.	Existing RFP Clause	Amended Clause
		28	executed and inspected, of the following Operating Systems (32 and 64 bit) : Win XP, Win7, Win8.x, Win10.x, Server 2008 R2, 2012 R2, Linux, Solaris10, Redhat 5 & Above, Unix and MAC OS, all industry standard OS. This requirement should be based on virtual execution and should not be Hardware or chipbased function	executed and inspected, of the Windows Operating Systems (32 and 64 bit) This requirement should be based on virtual execution and should not be Hardware or chip based function
27	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 29	Solution should have option to upload custom sandbox image running in Bank"s environment.	Solution should have option to upload/create custom sandbox image running in Bank's environment.
28	47	Technical Specifications Network Anti-APT, Clause No. 30	The sandbox must have the capability to analyze large files and must be able to support more than 50MB file size and following File type supports (.doc, .xls, .ppt, .pdf, .exe, .zip, .rar, .tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .arj, .exe, .dll, .avi, .mpeg, .mp3/4, .jpg, java script, JavaArchive JAR, LNK, .chm, .swf, .sys, .com, .hwp, etc.)	The sandbox must have the capability to analyze large files and must be able to support different file size and following File type supports (.doc, .xls, .ppt, .pdf, .exe, .zip, .rar, .tar, .gz, .tar.gz, .tgz, .zip, .bz2, .tar.bz2, .bz, .tar.Z, .cab, .rar, .exe, .dll, .jpg, java script, JavaArchive JAR, LNK, .swf, .sys, .com, .hwp, etc.)
29	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 34	Solution must inspect SMTP, POP3, IMAP traffic, UDP traffic, Proxy/http traffic, DNS traffic, Non-standard TCP port traffic	Solution must inspect UDP traffic, Proxy/http traffic, DNS traffic, Non-standard TCP port traffic
30	48	Technical Specification Point 39	Hardware should have minimum capacity of 4 TB	Clause Stands Deleted
31	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 41	Solution should track the infection or threat history for a device, with the ability to access all forensic evidence for past infections. (6 months)	Solution should track the infection or threat history for a device, with the ability to access all forensic evidence for past one month and should have minimum hardware capacity to store the same.
32	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 42	The solution should support hostname resolution through either Net Bios Lookup or reverse DNS. (Asset Identification)	Clause stands deleted
33	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 58	The solution should be able to capture packets for deep dive analysis and should support remote packet capturing for Kerberos traffic from the remote location for analysis. The	The solution should be able to capture packets for deep dive analysis and should support packet capturing for Kerberos traffic for analysis. The solution should store packet captures (PCAP) of

Sr. No.	Page No.	RFP Clause Name & No.	Existing RFP Clause	Amended Clause
			solution should store packet captures (PCAP) of all Malicious communications detected by sandbox and should have the ability to capture, publish and download PCAP files.	all Malicious communications detected by sandbox and should have the ability to capture, publish and download PCAP files.
34	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 61	<ul style="list-style-type: none"> for devices that are mobile (outside of network perimeter defenses) on split-tunnel VPN connections. 	Clause stands Deleted
35	49	ANNEXURE-XII / Network Anti-APT Solution & 61	using P2P Malicious Communications such as Zero Access, TDL4, Zeus V3, and Sality (The solution should identify such malicious softwares like Sality, etc.)	using P2P Malicious Communications such as Zero Access/TDL4/Zeus V3/ Sality (The solution should identify such malicious softwares like Sality, etc.)
36	49	Technical Specifications Network Anti-APT, Clause No. 61	· beyond just the initial dropper and be able to identify successful communicated to C & C server and successful malware execution on Endpoint.	· beyond just the initial dropper and be able to identify successful communicated to C & C server and successful malware execution on Endpoint, if integrated with Endpoint ATP.
37	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 62	Solution should provide administrators with the ability to view file download activity associated with infected Endpoint for a window of time prior to the determination of the endpoint's infected status.	Solution should provide administrators with the ability to view file download activity associated with infected Endpoint for a window of time prior to the determination of the endpoint's infected status, if integrated with endpoint ATP.
38	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 64	The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web, the suspicious mail attachment and internal infections.	The proposed solution should be able to inspect the multi-protocol sessions to detect and flag the suspicious activity including suspicious file downloads through the web.
39	49	Technical Specifications Network Anti-APT, Clause No. 67	The proposed solution should provide Geo location intelligence for (malware sources, network exploit sources, document exploit sources, malware c&c destinations) and should control traffic based on geographical locations.	Clause stands deleted
40	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 76	The proposed solution should support Multiple protocols inspection. Example :- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction :SMB ,Database protocol (MySQL, MSSQL, Oracle) on a single device	Clause stands deleted

Sr. No.	Page No.	RFP Clause Name & No.	Existing RFP Clause	Amended Clause
41	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 78	The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.	Clause stands deleted
42	50	Technical Specification Point 80	Solution should correlate events and differentiate between a confirm infection and a suspicious event, thereby pinpointing infected devices accurately.	Solution should correlate events and differentiate between a confirm infection and a suspicious event, thereby pinpointing infected devices accurately, if integrated with endpoint ATP
43	50	Technical Specifications Network Anti-APT, Clause No. 89	Solution should provide a conviction engine that aggregates evidence and determines the presence of a threat on a device.	Solution should provide a conviction engine that aggregates evidence and determines the presence of a threat on a device, if integrated with endpoint ATP
44	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 95	Solutions should allow for incidents to be marked, tagged and acknowledged and should be able to mark assets/host	Solutions should allow for incidents to be marked, tagged and acknowledged and should be able to mark assets/host, if integrated with Incident Management Solution
45	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 96	Solutions should allow a user to track investigation efforts at an asset/device level by supporting tagging/notes, marking assets and threats as remediated, and support auto-expiration if no further evidence has been collected for a period of time.	Solutions should allow a user to track investigation efforts at an asset/device level by supporting tagging/notes, marking assets and threats as remediated, and support auto-expiration if no further evidence has been collected for a period of time, if integrated with Incident Management Solution
46	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 101	Solution should allow for categorization of devices along with level of importance,, of those devices should they be infected, with the following priority:- Critical, High, Medium, Low	Solution should allow for categorization of alerts with the following priority:- Critical, High, Medium, Low
47	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 102	Solution must provide infection forensics to enable incident responders to validate findings and adapt security policy (connection attempt counts, connection attempt success, bytes in, bytes out, full packet captures, suspicious file static and dynamic analysis, Forensic Metadata and Infection Forensics)	Clause stands deleted
48	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 106	Solution should be able to perform DNS redirection for malicious DNS queries, to prohibit infections from communicating with cyber criminals.	Clause stands deleted
49	52	ANNEXURE-XII /	The solution should provide the ability to	The solution should provide the ability to upload

Sr. No.	Page No.	RFP Clause Name & No.	Existing RFP Clause	Amended Clause
		Network Anti-APT Solution & 117	upload and analyze objects through a collection of custom virtual machines rather than a generic image.	and analyze objects within VMs
50	52	Technical Specifications Network Anti-APT, Clause No. 119	The solution should provide a detailed list of every DLL and API referenced, all header information about the binary, and complete assembly-language listing of the binary code.	The solution should provide a detailed list of every DLL and API referenced, all header information about the binary.
51	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 120	The solution should provide the ability to upload gold image and analyze threats under conditions of actual host environment.	Clause Stands deleted
52	45 - 52	Annexure XII - Network Anti-APT Solution Technical Specification Clause no 123	The Anti-APT Solution should have minimum 50 Sandboxes and should be able to handle at least 25000 files in a day	The Anti-APT Solution should have minimum 50 Sandboxes and should be able to handle at least 5000 files in a day