Response to Pre Bid Queries - RFP for Procurement of Breach & Attack Simulation Solution NPCI/RFP/2022-23/IT/03 dated 29.06.2022							
Sr. No.	**Document Reference**	**Page No**	**Clause No**	**Description in RFP**	**Clarification Sought**	**Additional Remarks (if any)**	**Response**
1	RFP-for-procurement-of-Breach & Attack Simulation Solution	**10**	3.1 - Scope of Work	· The bidder / OEM shall provide 24*7*365 basis post implementation technical support for the components supplied. Support center must be based in INDIA.		The bidder / OEM shall provide 24*5*365 basis post implementation technical support for the components supplied. Support center must be based in INDIA.	No Change in RFP Terms
2	RFP-for-procurement-of-Breach & Attack Simulation Solution	**23**	8.4 - Performance bank guarantee	The Successful bidder shall, within 14 working days of receipt of Purchase Order, submit a Performance Bank Guarantee (PBG) equal to 10% of total value of the Purchase order (exclusive of taxes), valid for term of the order.		The Successful bidder shall, within 14 working days of receipt of Purchase Order, submit a Performance Bank Guarantee (PBG) equal to 3% of total value of the Purchase order.	No Change in RFP
3	RFP-for-procurement-of-Breach & Attack Simulation Solution	**37**	Section 9 - Technical Specifications - point B2	For the proposed solution, If cloud based then all data collected/processed to be stored only in INDIA.	Are these two mutually exclusive Or they are mutually inclusive. We can understand that if the Cloud is not hosted in India(B2), are they asking for Separate instance dedicated for NPCI (B3).		This is mentioned as Good to Have. Mutually inclusive with Section 9 - Technical Specifications - point B3
4	RFP-for-procurement-of-Breach & Attack Simulation Solution	**37**	Section 9 - Technical Specifications - point B3	For the proposed solution, If cloud based then all data collected/processed should be secure in a separate cloud instance, dedicated for NPCI.			This is mentioned as Must Have. Mutually inclusive with Section 9 - Technical Specifications - point B2
5	RFP-for-procurement-of-Breach & Attack Simulation Solution	**37**	Section 9 - Technical Specifications - Point B2	If cloud based….	Are above clauses applicable if solution is hybrid, ? so some data is processed at agent level, and reports are processed at cloud end dedicated to their account		Yes, Applicable for Hybrid Solution.
6	RFP-for-procurement-of-Breach & Attack Simulation Solution	**37**	Section 9 - Technical Specifications - point - B3	If cloud based….	Are above clauses applicable if solution is hybrid, ? so some data is processed at agent level, and reports are processed at cloud end dedicated to their account		Yes, Applicable for Hybrid Solution.
7	RFP-for-procurement-of-Breach & Attack Simulation Solution	**37**	Section 9 - Technical Specifications - point B2 and Be	all data collected	What if there is No customer Data is collected. Only test cases are tested for success or failure, you still need to comply for above ?		Yes. No change in RFP Terms.

8	RFP-for-procurement-of-Breach & Attack Simulation Solution	**37**	Section 9 - Technical Specifications - point B2 and Be	all data collected	If the real data collected of NPCI remains inside the NPCI network then should B2 and B3 are required ?		Yes. No change in RFP Terms.
9	RFP-for-procurement-of-Breach & Attack Simulation Solution	**37**	Section 9 - Technical Specifications - point C1	The solution must directly integrate with common commercial SIEM solutions	Kindly name the SIEM that is used.		Solution should be Vendor Agnostic. No change in RFP Terms
10	RFP-for-procurement-of-Breach & Attack Simulation Solution	**37**	Section 9 - Technical Specifications - point C2	The solution must directly integrate with common commercial endpoint security controls	Name endpoint controls used by NPCI		Solution should be Vendor Agnostic. No change in RFP Terms
11	RFP-for-procurement-of-Breach & Attack Simulation Solution	**39**	Section 9 - Technical Specifications - point D25	The Solution should provide POA (Proof of acceptance) for manual assessments / simulation along with Mitigation steps	POA should be proof of attack an not proof of acceptance correct ?		Refer to Corrigendum - 1
12	RFP-for-procurement-of-Breach & Attack Simulation Solution	**39**	Section 9 - Technical Specifications - point D31	The solution should provide technology vendor-specific remediation signatures and prioritization as mitigation recommendations	Are these remediation signatures or remediation guidelines ?		Refer to Corrigendum - 1
13	RFP-for-procurement-of-Breach & Attack Simulation Solution	37	B2	For the proposed solution, If cloud based then all data collected/processed to be stored only in INDIA.	Are these two mutually exclusive Or they are mutually inclusive. We can understand that if the Cloud is not hosted in India(B2), are they asking for Separate instance dedicated for NPCI (B3).		This is mentioned as Good to Have. Mutually inclusive with Section 9 - Technical Specifications - point B3
14	RFP-for-procurement-of-Breach & Attack Simulation Solution	37	B3	For the proposed solution, If cloud based then all data collected/processed should be secure in a separate cloud instance, dedicated for NPCI.			This is mentioned as Must Have. Mutually inclusive with Section 9 - Technical Specifications - point B2
15	RFP-for-procurement-of-Breach & Attack Simulation Solution	37	B2	If cloud based….	Are above clauses applicable if solution is hybrid, ? so some data is processed at agent level, and reports are processed at cloud end dedicated to their account		Yes, Applicable for Hybrid Solution.
16	RFP-for-procurement-of-Breach & Attack Simulation Solution	37	B3	If cloud based….	Are above clauses applicable if solution is hybrid, ? so some data is processed at agent level, and reports are processed at cloud end dedicated to their account		Yes, Applicable for Hybrid Solution.

17	RFP-for-procurement-of-Breach & Attack Simulation Solution	37	B2 and Be	all data collected	What if there is No customer Data is collected. Only test cases are tested for success or failure, you still need to comply for above ?		Yes. No change in RFP Terms.
18	RFP-for-procurement-of-Breach & Attack Simulation Solution	37	B2 and Be	all data collected	If the real data collected of NPCI remains inside the NPCI network then should B2 and B3 are required ?		Yes. No change in RFP Terms.
19	RFP-for-procurement-of-Breach & Attack Simulation Solution	37	C1	The solution must directly integrate with common commercial SIEM solutions	Kindly name the SIEM that is used.		Solution should be Vendor Agnostic. No change in RFP Terms
20	RFP-for-procurement-of-Breach & Attack Simulation Solution	37	C2	The solution must directly integrate with common commercial endpoint security controls	Name endpoint controls used by NPCI		Solution should be Vendor Agnostic. No change in RFP Terms
21	RFP-for-procurement-of-Breach & Attack Simulation Solution	39	D25	The Solution should provide POA (Proof of acceptance) for manual assessments / simulation along with Mitigation steps	POA should be proof of attack an not proof of acceptance correct ?		Refer to Corrigendum - 1
22	RFP-for-procurement-of-Breach & Attack Simulation Solution	39	D31	The solution should provide technology vendor-specific remediation signatures and prioritization as mitigation recommendations	Are these remediation signatures or remediation guidelines ?		Refer to Corrigendum - 1
23	RFP-for-procurement-of-Breach & Attack Simulation Solution	37	C1	The solution must directly integrate with common commercial SIEM solutions	Kindly name the SIEM that is used.		Solution should be Vendor Agnostic. No change in RFP Terms
24	RFP-for-procurement-of-Breach & Attack Simulation Solution	37	C2	The solution must directly integrate with common commercial endpoint security controls	Name endpoint controls used by NPCI		Solution should be Vendor Agnostic. No change in RFP Terms
25	RFP-for-procurement-of-Breach & Attack Simulation Solution	39	D25	The Solution should provide POA (Proof of acceptance) for manual assessments / simulation along with Mitigation steps	POA should be proof of attack an not proof of acceptance correct ?		Refer to Corrigendum - 1
26	RFP-for-procurement-of-Breach & Attack Simulation Solution	39	D31	The solution should provide technology vendor-specific remediation signatures and prioritization as mitigation recommendations	Are these remediation signatures or remediation guidelines ?		Refer to Corrigendum - 1

27	RFP Document	37	B2	For the proposed solution, If cloud based then all data collected/processed to be stored only in INDIA.	Are these two mutually exclusive Or they are mutually inclusive. We can understand that if the Cloud is not hosted in India(B2), are they asking for Separate instance dedicated for NPCI (B3).		This is mentioned as Good to Have. Mutually inclusive with Section 9 - Technical Specifications - point B3
28	RFP Document	37	B3	For the proposed solution, If cloud based then all data collected/processed should be secure in a separate cloud instance, dedicated for NPCI.			This is mentioned as Must Have. Mutually inclusive with Section 9 - Technical Specifications - point B2
29	RFP Document	37	B2	If cloud based….	Are above clauses applicable if solution is hybrid, ? so some data is processed at agent level, and reports are processed at cloud end dedicated to their account		Yes, Applicable for Hybrid Solution.
30	RFP Document	37	B3	If cloud based….	Are above clauses applicable if solution is hybrid, ? so some data is processed at agent level, and reports are processed at cloud end dedicated to their account		Yes, Applicable for Hybrid Solution.
31	RFP Document	37	B2 and Be	All data collected	What if there is No customer Data is collected. Only test cases are tested for success or failure, you still need to comply for above ?		Yes. No change in RFP Terms.
32	RFP Document	37	B2 and Be	all data collected	If the real data collected of NPCI remains inside the NPCI network then should B2 and B3 are required ?		Yes. No change in RFP Terms.
33	RFP Document	37	C1	The solution must directly integrate with common commercial SIEM solutions	Kindly name the SIEM that is used.		Solution should be Vendor Agnostic. No change in RFP Terms
34	RFP Document	37	C2	The solution must directly integrate with common commercial endpoint security controls	Name endpoint controls used by NPCI		Solution should be Vendor Agnostic. No change in RFP Terms
35	RFP Document	39	D25	The Solution should provide POA (Proof of acceptance) for manual assessments / simulation along with Mitigation steps	POA should be proof of attack an not proof of acceptance correct ?		Refer to Corrigendum - 1
36	RFP Document	39	D31	The solution should provide technology vendor-specific remediation signatures and prioritization as mitigation recommendations	Are these remediation signatures or remediation guidelines ?		Refer to Corrigendum - 1

37	RFP Document	13	2	The bidder should have reported minimum annual turnover of Rs. 5 crores in each of the last 3 financial years and should have reported profits (profit after tax) as per audited financial statements in last 3 financial years (FY 2018-19, 2019-20, 2020-21).	We request you to amend the caluse as Due to Pandemic our Profit after Tax is not there in FY-20-21 however we have postive networth. In lockdown the profit after tax affected due to many reason. All other PSU BFSI considering this caluse and giving relaxation for FY20-21. PLease help to amend so that we can submit our BID.		No Change in RFP
38	RFP Document	21	1. Part – B Vendor Evaluation Matrix	Customer BFSI reference in India (Bidder & OEM) Please provide at least 2 India References including	Needs clarification as Customer in India BFSI reference (Bidder and OEM) has to give a combination of 2 POs or each one have to given 2 numbers of Pos.		No change in RFP Terms
39	RFP Document- Section 9	37	C6	The solution should have technical integrations available for specific vendors where applicable (e.g. SIEMs, ITSM's, ticketing systems, Vulnerability assessment tools, log management, Firewalls, SOAR, automation/orchestration, analytics platforms, threat intelligence platforms, etc.)	A Breach and attack simulation technology requires integration for common Detection/Protection technologies. Integration with other technologies like Vulnerability assessment, ITSM, ticketing system are just desirable features. Request NPCI to modify the point as "The solution should have technical integrations available with key security Prevention/Detection technologies."		Refer to Corrigendum - 1
40	RFP Document- Section 9	37	D2	The solution should include attacks simulations relevant to information technology targets, FinTech Targets, BFSI Targets, NBFC Targets.	Owing to the dynamic nature of attack by attackers a static template can never be used for any Industry vertical as the TTPs of the attackers keep evolving by the day. It is imperative to have the option of building customized template basis industry vertical, basis the content library published by OEM. Request NPCI to modify this point as "the solution should support creation of custom simulations relevant to FinTech Targets, BFSI Targets, NBFC Targets from the library of global attacks provided."		Refer to Corrigendum - 1
41	RFP Document- Section 9	38	D4	The solution must be able to Represent Vulnerability Risk scores (Low, Medium, High, Critical) based on proven cybersecurity risk assessment models. (e.g. DREAD, CVSSV3, NIST)	Risk Scores are majorly tracked by technologies that play into the Security Rating Service Space. BAS tools rate the findings on the basis of severity. Request NPCI to modify the point as, "The solution must be able to represent results of breach emulation on the basis of a severity using a visual representation tool like HEAT MAP, showing areas of strength and weaknesses as per the various phases of an attack lifecycle or be able to represent the technologies in terms of their percentage of detection (efficacy)"		No change in RFP Terms

42	RFP Document-Section 9	38	D8	Solution should have Ability to simulate Machine-based attacks - known vulnerabilities on internet facing systems, misconfiguration of network perimeter controls, exposed applications, etc.	Applications exposed to the Internet are normally controlled at an organizational level and in most cases are Web application. Request NPCI to modify the point as "Solution should have Ability to simulate Machine-based attacks - known vulnerabilities on internet-facing systems, misconfiguration of network perimeter controls and web based applications."		Refer to Corrigendum - 1
43	RFP Document-Section 9	38	D13	Solution should support Endpoint Assessment - test security state of endpoints by comprehensively testing: automated behavioural detection (EDR), signature-based detection (anti-virus), known vulnerabilities including Windows patches.	Vulnerability patching is normally tracked as part of patch management process and is outside the scope of a Breach and Attack Simulation solution. Request NPCI to modify the point to "Solution should support Data exfiltration attempt, such as file upload (Network data loss prevention (DLP test) "		Refer to Corrigendum - 1
44	RFP Document-Section 9	38	D18	Solution should support Data exfiltration attempt, such as file upload (Network data loss prevention (DLP test) on cloud drives (e.g. Gdrive, onedrive, dropbox, slack etc.)	Testing of dat exfiltration should not be restricted only to cloud storage services, Request NPCI to modify this to "Solution should support Data exfiltration attempt, such as file upload (Network data loss prevention (DLP test)"		Refer to Corrigendum - 1
45	RFP Document-Section 9	38	D31	The solution should provide technology vendor-specific remediation signatures and prioritization as mitigation recommendations	BAS solution by itself is not a detection or a prevention technology and the Basic outcome from a BAS/MSV solution is to identify detection inefficiencies, the remediation (from control perspective) however, needs to be done by a respective OEM vendor. Request NPCI to rephrase this point as : " The solution should provide Possible Detection alert name along with Mitre mitigation recommendations."		Refer to Corrigendum - 1
46	RFP Document-Section 9	38	D34	The Supplier should validate and measure the detection and response capabilities of security pipelines and detection analysts in the SOC	Request NPCI to reconsider this point, as Validating and measuring detection and response capabilities of security pipelines and detection analyst (covering aspects outside of technology) in the SOC are achieved through Consulting services Engagements.		Refer to Corrigendum - 1
47	RFP Document-Section 9	38	D37	The Supplier should support processes to request and run network penetration tests against the service and report the results.	Request NPCI to reconsider and remove this point, as the Penetration test requirement falls outside the scope of attack emulation as PT also covers Application testing. No Emulation tests can substitute the need for a Penetration test		Requirement is mentioned as Good to Have. No change in RFP Terms.
48	RFP Document-Section 9	38	D41	The solution should supports Azure & AWS cloud endpoints.	Request NPCI to specify what Operating System Azure & AWS Cloud end points are running on currently.		Operating System Support as per RFP Ask in Section 9 - Technical Specifications Point A2

49	RFP Document-Section 9	38	D42	The solution should support use cases specific to Kubernetes, Docker, Container deployments	Request NPCI to specify use cases pertaining to Kubernetes, Docker, Container deployments		Refer to Corrigendum - 1
50	RFP Document-Section 9	37	C6	The solution should have technical integrations available for specific vendors where applicable (e.g. SIEMs, ITSM's, ticketing systems, Vulnerability assessment tools, log management, Firewalls, SOAR, automation/orchestration, analytics platforms, threat intelligence platforms, etc.)	A Breach and attack simulation technology requires integration for common Detection/Protection technologies. Integration with other technologies like Vulnerability assessment, ITSM, ticketing system are just desirable features. Request NPCI to modify the point as "The solution should have technical integrations available with key security Prevention/Detection technologies."		Refer to Corrigendum - 1
51	RFP Document-Section 9	37	D2	The solution should include attacks simulations relevant to information technology targets, FinTech Targets, BFSI Targets, NBFC Targets.	Owing to the dynamic nature of attack by attackers a static template can never be used for any Industry vertical as the TTPs of the attackers keep evolving by the day. It is imperative to have the option of building customized template basis industry vertical, basis the content library published by OEM. Request NPCI to modify this point as "the solution should support creation of custom simulations relevant to FinTech Targets, BFSI Targets, NBFC Targets from the library of global attacks provided."		Refer to Corrigendum - 1
52	RFP Document-Section 9	38	D4	The solution must be able to Represent Vulnerability Risk scores (Low, Medium, High, Critical) based on proven cybersecurity risk assessment models. (e.g. DREAD, CVSSV3, NIST)	Risk Scores are majorly tracked by technologies that play into the Security Rating Service Space. BAS tools rate the findings on the basis of severity. Request NPCI to modify the point as, "The solution must be able to represent results of breach emulation on the basis of a severity using a visual representation tool like HEAT MAP, showing areas of strength and weaknesses as per the various phases of an attack lifecycle or be able to represent the technologies in terms of their percentage of detection (efficacy)"		No change in RFP Terms
53	RFP Document-Section 9	38	D8	Solution should have Ability to simulate Machine-based attacks - known vulnerabilities on internet facing systems, misconfiguration of network perimeter controls, exposed applications, etc.	Applications exposed to the Internet are normally controlled at an organizational level and in most cases are Web application. Request NPCI to modify the point as "Solution should have Ability to simulate Machine-based attacks - known vulnerabilities on internet-facing systems, misconfiguration of network perimeter controls and web based applications."		Refer to Corrigendum - 1

54	RFP Document-Section 9	38	D13	Solution should support Endpoint Assessment - test security state of endpoints by comprehensively testing: automated behavioural detection (EDR), signature-based detection (anti-virus), known vulnerabilities including Windows patches.	Vulnerability patching is normally tracked as part of patch management process and is outside the scope of a Breach and Attack Simulation solution. Request NPCI to modify the point to "Solution should support Data exfiltration attempt, such as file upload (Network data loss prevention (DLP test) "		Refer to Corrigendum - 1
55	RFP Document-Section 9	38	D18	Solution should support Data exfiltration attempt, such as file upload (Network data loss prevention (DLP test) on cloud drives (e.g. Gdrive, onedrive, dropbox, slack etc.)	Testing of dat exfiltration should not be restricted only to cloud storage services, Request NPCI to modify this to "Solution should support Data exfiltration attempt, such as file upload (Network data loss prevention (DLP test)"		Refer to Corrigendum - 1
56	RFP Document-Section 9	38	D31	The solution should provide technology vendor-specific remediation signatures and prioritization as mitigation recommendations	BAS solution by itself is not a detection or a prevention technology and the Basic outcome from a BAS/MSV solution is to identify detection inefficiencies, the remediation (from control perspective) however, needs to be done by a respective OEM vendor. Request NPCI to rephrase this point as : " The solution should provide Possible Detection alert name along with Mitre mitigation recommendations."		Refer to Corrigendum - 1
57	RFP Document-Section 9	38	D34	The Supplier should validate and measure the detection and response capabilities of security pipelines and detection analysts in the SOC	Request NPCI to reconsider this point, as Validating and measuring detection and response capabilities of security pipelines and detection analyst (covering aspects outside of technology) in the SOC are achieved through Consulting services Engagements.		Refer to Corrigendum - 1
58	RFP Document-Section 9	38	D37	The Supplier should support processes to request and run network penetration tests against the service and report the results.	Request NPCI to reconsider and remove this point, as the Penetration test requirement falls outside the scope of attack emulation as PT also covers Application testing. No Emulation tests can substitute the need for a Penetration test		Requirement is mentioned as Good to Have. No change in RFP Terms.
59	RFP Document-Section 9	38	D41	The solution should supports Azure & AWS cloud endpoints.	Request NPCI to specify what Operating System Azure & AWS Cloud end points are running on currently.		Operating System Support as per RFP Ask in Section 9 - Technical Specifications Point A2
60	RFP Document-Section 9	38	D42	The solution should support use cases specific to Kubernetes, Docker, Container deployments	Request NPCI to specify use cases pertaining to Kubernetes, Docker, Container deployments		Refer to Corrigendum - 1

61	RFP Document-Section 9	37	C6	The solution should have technical integrations available for specific vendors where applicable (e.g. SIEMs, ITSM's, ticketing systems, Vulnerability assessment tools, log management, Firewalls, SOAR, automation/orchestration, analytics platforms, threat intelligence platforms, etc.)	A Breach and attack simulation technology requires integration for common Detection/Protection technologies. Integration with other technologies like Vulnerability assessment, ITSM, ticketing system are just desirable features. Request NPCI to modify the point as "The solution should have technical integrations available with key security Prevention/Detection technologies."		Refer to Corrigendum - 1
62	RFP Document-Section 9	37	D2	The solution should include attacks simulations relevant to information technology targets, FinTech Targets, BFSI Targets, NBFC Targets.	Owing to the dynamic nature of attack by attackers a static template can never be used for any Industry vertical as the TTPs of the attackers keep evolving by the day. It is imperative to have the option of building customized template basis industry vertical, basis the content library published by OEM. Request NPCI to modify this point as "the solution should support creation of custom simulations relevant to FinTech Targets, BFSI Targets, NBFC Targets from the library of global attacks provided."		Refer to Corrigendum - 1
63	RFP Document-Section 9	38	D4	The solution must be able to Represent Vulnerability Risk scores (Low, Medium, High, Critical) based on proven cybersecurity risk assessment models. (e.g. DREAD, CVSSV3, NIST)	Risk Scores are majorly tracked by technologies that play into the Security Rating Service Space. BAS tools rate the findings on the basis of severity. Request NPCI to modify the point as, "The solution must be able to represent results of breach emulation on the basis of a severity using a visual representation tool like HEAT MAP, showing areas of strength and weaknesses as per the various phases of an attack lifecycle or be able to represent the technologies in terms of their percentage of detection (efficacy)"		No change in RFP Terms
64	RFP Document-Section 9	38	D8	Solution should have Ability to simulate Machine-based attacks - known vulnerabilities on internet facing systems, misconfiguration of network perimeter controls, exposed applications, etc.	Applications exposed to the Internet are normally controlled at an organizational level and in most cases are Web application. Request NPCI to modify the point as "Solution should have Ability to simulate Machine-based attacks - known vulnerabilities on internet-facing systems, misconfiguration of network perimeter controls and web based applications."		Refer to Corrigendum - 1
65	RFP Document-Section 9	38	D13	Solution should support Endpoint Assessment - test security state of endpoints by comprehensively testing: automated behavioural detection (EDR), signature-based detection (anti-virus), known vulnerabilities including Windows patches.	Vulnerability patching is normally tracked as part of patch management process and is outside the scope of a Breach and Attack Simulation solution. Request NPCI to modify the point to "Solution should support Data exfiltration attempt, such as file upload (Network data loss prevention (DLP test) "		Refer to Corrigendum - 1

66	RFP Document-Section 9	38	D18	Solution should support Data exfiltration attempt, such as file upload (Network data loss prevention (DLP test) on cloud drives (e.g. Gdrive, onedrive, dropbox, slack etc.)	Testing of dat exfiltration should not be restricted only to cloud storage services, Request NPCI to modify this to "Solution should support Data exfiltration attempt, such as file upload (Network data loss prevention (DLP test)"		Refer to Corrigendum - 1
67	RFP Document-Section 9	38	D31	The solution should provide technology vendor-specific remediation signatures and prioritization as mitigation recommendations	BAS solution by itself is not a detection or a prevention technology and the Basic outcome from a BAS/MSV solution is to identify detection inefficiencies, the remediation (from control perspective) however, needs to be done by a respective OEM vendor. Request NPCI to rephrase this point as : " The solution should provide Possible Detection alert name along with Mitre mitigation recommendations."		Refer to Corrigendum - 1
68	RFP Document-Section 9	38	D34	The Supplier should validate and measure the detection and response capabilities of security pipelines and detection analysts in the SOC	Request NPCI to reconsider this point, as Validating and measuring detection and response capabilities of security pipelines and detection analyst (covering aspects outside of technology) in the SOC are achieved through Consulting services Engagements.		Refer to Corrigendum - 1
69	RFP Document-Section 9	38	D37	The Supplier should support processes to request and run network penetration tests against the service and report the results.	Request NPCI to reconsider and remove this point, as the Penetration test requirement falls outside the scope of attack emulation as PT also covers Application testing. No Emulation tests can substitute the need for a Penetration test		Requirement is mentioned as Good to Have. No change in RFP Terms.
70	RFP Document-Section 9	38	D41	The solution should supports Azure & AWS cloud endpoints.	Request NPCI to specify what Operating System Azure & AWS Cloud end points are running on currently.		Operating System Support as per RFP Ask in Section 9 - Technical Specifications Point A2
71	RFP Document-Section 9	38	D42	The solution should support use cases specific to Kubernetes, Docker, Container deployments	Request NPCI to specify use cases pertaining to Kubernetes, Docker, Container deployments		Refer to Corrigendum - 1
72	**Section 9 - Technical Specifications**	**Page 37**	**A3. Section 9 - Technical Specifications**	The solution must support proxy communications to the Internet. Simulation Agents installed must support proxy communications to the Breach & Attack simulation solution's cloud platform counterpart.	**Please specify for Which type of proxy, an implicit or explicit proxy, is used at NPCI?**		Solution should be Proxy OEM Agnostic & Proxy Solution Architecture Agnostic. No change in RFP Terms.
73	**Section 9 - Technical Specifications**	**Page 37**	**A4.Section 9 - Technical Specifications**	The Solution agent component must be installable as a software package (Publishing it through group policy) and an image/Golden image.	**Please elaborate on question What type of security control BAS will be focusing on a few system UAT/dedicated systems or in any security zone?**		No Change in RFP Terms

74	**Section 9 - Technical Specifications**	**Page 37**	**A7.Section 9 - Technical Specifications**	For the proposed Solution, All installed agents/simulators should have capability to run assessments/simulations as local user privilege and/or admin user privilege	**Please explain the difference between point A7 and point B7**		No Change in RFP Terms
75	**Section 9 - Technical Specifications**	**Page 37**	**B7.Section 9 - Technical Specifications**	The solution must include discrete privileged and user account levels with specific permissions for each (e.g. RBAC)	**Please explain the difference between point A7 and point B7**		No Change in RFP Terms
76	**Section 9 - Technical Specifications**	**Page 37**	**C1.Section 9 - Technical Specifications**	The solution must directly integrate with common commercial SIEM solutions	**We need to know what SIEM tool or solution NPCI is using.**		Solution should be Vendor Agnostic. No change in RFP Terms
77	**Section 9 - Technical Specifications**	**Page 37**	**C2.Section 9 - Technical Specifications**	The solution must directly integrate with common commercial endpoint security controls	**We require inputs; which endpoint tool or solution NPCI is using?**		Solution should be Vendor Agnostic. No change in RFP Terms
78	**Section 9 - Technical Specifications**	**Page 38**	**C3.Section 9 - Technical Specifications**	The solution must validate network security control effectiveness.	**Need further clarification on this point, namely the kind of security controls used in the NPCI network.**		The Solution should be Vendor Agnostic. No change in RFP Terms.
79	**Section 9 - Technical Specifications**	**Page 38**	**C4.Section 9 - Technical Specifications**	The solution must validate email security control effectiveness.	**We need further clarification on this point; is NPCI using a specific email security?**		Breach attack simulation use cases related to email security should be vendor agnostic. No change in RFP Terms
80	**Section 9 - Technical Specifications**	**Page 38**	**D4.Section 9 - Technical Specifications**	The solution must be able to Represent Vulnerability Risk scores (Low, Medium, High, Critical) based on proven cybersecurity risk assessment models. (e.g. DREAD, CVSSV3, NIST)	**NPCI is seeking for all of these or any one of them in terms of risk scoring? (DREAD, CVSSV3, NIST)**		No change in RFP Terms
81	**Section 9 - Technical Specifications**	**Page 38**	**D7.Section 9 - Technical Specifications**	Solution should have Ability to simulate Infiltration techniques for breaching a network or infecting a host - Via Email, Web & WAF.	**This appears to be a pen testing test case; it is outside the purview of BAS technology. Please elaborate.**		No change in RFP Terms

82	**Section 9 - Technical Specifications**	**Page 38**	**D10.Section 9 - Technical Specifications**	Solution should have Ability to test attacker lateral movement through a single machine (once successfully within a network) - e.g., brute force or pass-the-hash techniques to steal credentials for sensitive servers, moving across network segments in search for valuable data	**Please clarify on this point, which appears to be a test case for pen testing and falls outside the purview of BAS technology.**		No change in RFP Terms
83	**Section 9 - Technical Specifications**	**Page 38**	**D16.Section 9 - Technical Specifications**	Solution should support Transfer and/or execution of malware on a test system (Endpoint malware download and execution test)	**Please clarify on this point, which appears to be a test case for pen testing and is outside the scope of BAS technology.**		This is a Malware attack simulation Test Case. No change in RFP Terms.
84	**Section 9 - Technical Specifications**	**Page 39**	**D20.Section 9 - Technical Specifications**	Solution should support Proxy tests - HTTP/HTTPS inbound/outbound exposure to malicious or compromised websites (web malware, malicious scripts)	**Need additional clarification on this subject**		No change in RFP Terms
85	**Section 9 - Technical Specifications**	**Page 39**	**D3.2Section 9 - Technical Specifications**	The Supplier proposed solution should have capabilities to allow for the detection or prevention of unauthorized modification of data.	**Need additional clarification on this subject**		This is a FIM use case. No change in RFP Terms
86	**Section 9 - Technical Specifications**	**Page 39**	**D33.Section 9 - Technical Specifications**	Solution should able to do a lateral movement assessment from a single endpoint	**Please clarify on this point, which appears to be a test case for pen testing and is outside the scope of BAS technology.**		This is a Good to have Requirement.No change in RFP Terms.
87	**Section 9 - Technical Specifications**	**Page 39**	**D37.Section 9 - Technical Specifications**	The Supplier should support processes to request and run network penetration tests against the service and report the results.	**This point needs more clarification.**		Requirement is mentioned as Good to Have. No change in RFP Terms.
88	**Section 9 - Technical Specifications**	**Page 39**	**D39.Section 9 - Technical Specifications**	Solution should have integrated Email phishing simulation module	**This point needs more clarification.**		This is Email Security Use case. No change in RFP Terms.
89	**Section 9 - Technical Specifications**	**Page 39**	**D42.Section 9 - Technical Specifications**	The solution should support use cases specific to Kubernetes, Docker, Container deployments	**Could you please elaborate on if NPCI has a Kubernetes cluster for which security needs to be validated?**		Refer to Corrigendum - 1
90	**Section 9 - Technical Specifications**	**Page 40**	**E6.Section 9 - Technical Specifications**	The API must include support for both JSON and XML formats	**Does NPCI still use XML, or does it exclusively use JSON?**		No Change in RFP Terms

91	Section 9 - Technical Specifications	35	Infrastructure & Deployment, A3	The solution must support proxy communications to the Internet. Simulation Agents installed must support proxy communications to the Breach & Attack simulation solution's cloud platform counterpart.	Please specify for Which type of proxy, an implicit or explicit proxy, is used at NPCI?	Architecture Details are needed	Solution should be Proxy OEM Agnostic & Proxy Solution Architecture Agnostic. No change in RFP Terms.
92	Section 9 - Technical Specifications	35	Infrastructure & Deployment, A4	The Solution agent component must be installable as a software package (Publishing it through group policy) and an image/Golden image.	Please elaborate on question What type of security control BAS will be focusing on a few system UAT/dedicated systems or in any security zone?		No Change in RFP Terms
93	Section 9 - Technical Specifications	35	Infrastructure & Deployment, A7	For the proposed Solution, All installed agents/simulators should have capability to run assessments/simulations as local user privilege and/or admin user privilege	Please explain the difference between point A7 and point B7		No Change in RFP Terms
94	Section 9 - Technical Specifications	35	Solution Security & Compliance, B7	The solution must include discrete privileged and user account levels with specific permissions for each (e.g. RBAC)	Please explain the difference between point A7 and point B7		No Change in RFP Terms
95	Section 9 - Technical Specifications	35	Security Solutions Support & Integration, C1	The solution must directly integrate with common commercial SIEM solutions	We need to know what SIEM tool or solution NPCI is using.	Architecture Details are needed	Solution should be Vendor Agnostic. No change in RFP Terms
96	Section 9 - Technical Specifications	35	Security Solutions Support & Integration, C2	The solution must directly integrate with common commercial endpoint security controls	We require inputs; which endpoint tool or solution NPCI is using?		Solution should be Vendor Agnostic. No change in RFP Terms
97	Section 9 - Technical Specifications	36	Security Solutions Support & Integration, C3	The solution must validate network security control effectiveness.	Need further clarification on this point, namely the kind of security controls used in the NPCI network.		The Solution should be Vendor Agnostic. No change in RFP Terms.
98	Section 9 - Technical Specifications	36	Security Solutions Support & Integration, C4	The solution must validate email security control effectiveness.	We need further clarification on this point; is NPCI using a specific email security?		Breach attack simulation use cases related to email security should be vendor agnostic. No change in RFP Terms
99	Section 9 - Technical Specifications	36	Use Cases Support, D4	The solution must be able to Represent Vulnerability Risk scores (Low, Medium, High, Critical) based on proven cybersecurity risk assessment models. (e.g. DREAD, CVSSV3, NIST)	NPCI is seeking for all of these or any one of them in terms of risk scoring? (DREAD, CVSSV3, NIST)		No change in RFP Terms

100	Section 9 - Technical Specifications	36	Use Cases Support, D7	Solution should have Ability to simulate Infiltration techniques for breaching a network or infecting a host - Via Email, Web & WAF.	This appears to be a pen testing test case; it is outside the purview of BAS technology. Please elaborate.		No change in RFP Terms
101	Section 9 - Technical Specifications	36	Use Cases Support, D10	Solution should have Ability to test attacker lateral movement through a single machine (once successfully within a network) - e.g., brute force or pass-the-hash techniques to steal credentials for sensitive servers, moving across network segments in search for valuable data	Please clarify on this point, which appears to be a test case for pen testing and falls outside the purview of BAS technology.		No change in RFP Terms
102	Section 9 - Technical Specifications	36	Use Cases Support, D16	Solution should support Transfer and/or execution of malware on a test system (Endpoint malware download and execution test)	Please clarify on this point, which appears to be a test case for pen testing and is outside the scope of BAS technology.		This is a Malware attack simulation Test Case. No change in RFP Terms.
103	Section 9 - Technical Specifications	36	Use Cases Support, D20	Solution should support Proxy tests - HTTP/HTTPS inbound/outbound exposure to malicious or compromised websites (web malware, malicious scripts)	Need additional clarification on this subject		No change in RFP Terms
104	Section 9 - Technical Specifications	36	Use Cases Support, D32	The Supplier proposed solution should have capabilities to allow for the detection or prevention of unauthorized modification of data.	Need additional clarification on this subject		This is a FIM use case. No change in RFP Terms
105	Section 9 - Technical Specifications	36	Use Cases Support, D33	Solution should able to do a lateral movement assessment from a single endpoint	Please clarify on this point, which appears to be a test case for pen testing and is outside the scope of BAS technology.		This is a Good to have Requirement.No change in RFP Terms.
106	Section 9 - Technical Specifications	36	Use Cases Support, D37	The Supplier should support processes to request and run network penetration tests against the service and report the results.	This point needs more clarification.		Requirement is mentioned as Good to Have. No change in RFP Terms.
107	Section 9 - Technical Specifications	36	Use Cases Support, D39	Solution should have integrated Email phishing simulation module	This point needs more clarification.		This is Email Security Use case. No change in RFP Terms.
108	Section 9 - Technical Specifications	36	Use Cases Support, D42	The solution should support use cases specific to Kubernetes, Docker, Container deployments	Could you please elaborate on if NPCI has a Kubernetes cluster for which security needs to be validated?		Refer to Corrigendum - 1

109	Section 9 - Technical Specifications	36	Dashboards, Reporting & Automation, E6	The API must include support for both JSON and XML formats	Does NPCI still use XML, or does it exclusively use JSON?		No Change in RFP Terms
110	Technical Scoring Matrix:	21	7.3 Technical Scoring	Customer BFSI reference in India (Bidder & OEM) Please provide at least 2 India References including customer name, etc.	We request you to change this clause as "Customer BFSI reference in India (Bidder or OEM) Please provide at least 2 India References including customer name, etc."		No change in RFP Terms
111	Technical Scoring Matrix:	21	7.3 Technical Scoring	Work experience in past (similar project)	We request yo to cosnider experince in IT projects / system integration / similar projects. OR also consider similar experience of Bidder / OEM.		No change in RFP Terms
112	Section 9 - Technical Specifications	Page 37	A3. Section 9 - Technical Specifications	The solution must support proxy communications to the Internet. Simulation Agents installed must support proxy communications to the Breach & Attack simulation solution's cloud platform counterpart.	Please specify for Which type of proxy, an implicit or explicit proxy, is used at NPCI?		Solution should be Proxy OEM Agnostic & Proxy Solution Architecture Agnostic. No change in RFP Terms.
113	Section 9 - Technical Specifications	Page 37	A4.Section 9 - Technical Specifications	The Solution agent component must be installable as a software package (Publishing it through group policy) and an image/Golden image.	Please elaborate on question What type of security control BAS will be focusing on a few system UAT/dedicated systems or in any security zone?		No Change in RFP Terms
114	Section 9 - Technical Specifications	Page 37	A7.Section 9 - Technical Specifications	For the proposed Solution, All installed agents/simulators should have capability to run assessments/simulations as local user privilege and/or admin user privilege	Please explain the difference between point A7 and point B7		No Change in RFP Terms
115	Section 9 - Technical Specifications	Page 37	B7.Section 9 - Technical Specifications	The solution must include discrete privileged and user account levels with specific permissions for each (e.g. RBAC)	Please explain the difference between point A7 and point B7		No Change in RFP Terms
116	Section 9 - Technical Specifications	Page 37	C1.Section 9 - Technical Specifications	The solution must directly integrate with common commercial SIEM solutions	We need to know what SIEM tool or solution NPCI is using.		Solution should be Vendor Agnostic. No change in RFP Terms
117	Section 9 - Technical Specifications	Page 37	C2.Section 9 - Technical Specifications	The solution must directly integrate with common commercial endpoint security controls	We require inputs; which endpoint tool or solution NPCI is using?		Solution should be Vendor Agnostic. No change in RFP Terms

118	Section 9 - Technical Specifications	Page 38	C3.Section 9 - Technical Specifications	The solution must validate network security control effectiveness.	Need further clarification on this point, namely the kind of security controls used in the NPCI network.		The Solution should be Vendor Agnostic. No change in RFP Terms.
119	Section 9 - Technical Specifications	Page 38	C4.Section 9 - Technical Specifications	The solution must validate email security control effectiveness.	We need further clarification on this point; is NPCI using a specific email security?		Breach attack simulation use cases related to email security should be vendor agnostic. No change in RFP Terms
120	Section 9 - Technical Specifications	Page 38	D4.Section 9 - Technical Specifications	The solution must be able to Represent Vulnerability Risk scores (Low, Medium, High, Critical) based on proven cybersecurity risk assessment models. (e.g. DREAD, CVSSV3, NIST)	NPCI is seeking for all of these or any one of them in terms of risk scoring? (DREAD, CVSSV3, NIST)		No change in RFP Terms
121	Section 9 - Technical Specifications	Page 38	D7.Section 9 - Technical Specifications	Solution should have Ability to simulate Infiltration techniques for breaching a network or infecting a host - Via Email, Web & WAF.	This appears to be a pen testing test case; it is outside the purview of BAS technology. Please elaborate.		No change in RFP Terms
122	Section 9 - Technical Specifications	Page 38	D10.Section 9 - Technical Specifications	Solution should have Ability to test attacker lateral movement through a single machine (once successfully within a network) - e.g., brute force or pass-the-hash techniques to steal credentials for sensitive servers, moving across network segments in search for valuable data	Please clarify on this point, which appears to be a test case for pen testing and falls outside the purview of BAS technology.		No change in RFP Terms
123	Section 9 - Technical Specifications	Page 38	D16.Section 9 - Technical Specifications	Solution should support Transfer and/or execution of malware on a test system (Endpoint malware download and execution test)	Please clarify on this point, which appears to be a test case for pen testing and is outside the scope of BAS technology.		This is a Malware attack simulation Test Case. No change in RFP Terms.
124	Section 9 - Technical Specifications	Page 39	D20.Section 9 - Technical Specifications	Solution should support Proxy tests - HTTP/HTTPS inbound/outbound exposure to malicious or compromised websites (web malware, malicious scripts)	Need additional clarification on this subject		No change in RFP Terms
125	Section 9 - Technical Specifications	Page 39	D3.2Section 9 - Technical Specifications	The Supplier proposed solution should have capabilities to allow for the detection or prevention of unauthorized modification of data.	Need additional clarification on this subject		This is a FIM use case. No change in RFP Terms

126	Section 9 - Technical Specifications	Page 39	D33.Section 9 - Technical Specifications	Solution should able to do a lateral movement assessment from a single endpoint	Please clarify on this point, which appears to be a test case for pen testing and is outside the scope of BAS technology.		This is a Good to have Requirement.No change in RFP Terms.
127	Section 9 - Technical Specifications	Page 39	D37.Section 9 - Technical Specifications	The Supplier should support processes to request and run network penetration tests against the service and report the results.	This point needs more clarification.		Requirement is mentioned as Good to Have. No change in RFP Terms.
128	Section 9 - Technical Specifications	Page 39	D39.Section 9 - Technical Specifications	Solution should have integrated Email phishing simulation module	This point needs more clarification.		This is Email Security Use case. No change in RFP Terms.
129	Section 9 - Technical Specifications	Page 39	D42.Section 9 - Technical Specifications	The solution should support use cases specific to Kubernetes, Docker, Container deployments	Could you please elaborate on if NPCI has a Kubernetes cluster for which security needs to be validated?		Refer to Corrigendum - 1
130	Section 9 - Technical Specifications	Page 40	E6.Section 9 - Technical Specifications	The API must include support for both JSON and XML formats	Does NPCI still use XML, or does it exclusively use JSON?		No Change in RFP Terms