

EVALUATION REPORT
(As Per Rule 35 of PP Rules, 2004)

1.	Name of Procuring Agency:	HQ NADRA Islamabad
2.	Method of Procurement:	Single Stage Two Envelope Method
3.	Title of Procurement:	Evaluation Report for Procurement of Subscription of Cyber Threat Intelligence Digital Risk
4.	Tender Inquiry No.:	NADRA-HQ-RFB-238/2023
5.	PPRA Ref. No. (TSE):	TS527479E
6.	Date & Time of Bid Closing:	28 th December, 2023 At 1100 Hrs
7.	Date & Time of Bid Opening:	28 th December, 2023 At 1130 Hrs
8.	No of Bids Received:	03 x Bids
9.	Criteria for Bid Evaluation:	As per Eligibility mentioned in Bidding Documents
10.	Details of Bid(s) Evaluation:	As under:-


Name of Bidder	Marks		Evaluated Cost	Rule/Regulation/SBD*/Policy/Basis for Rejection / Acceptance as per Rule 35 of PP Rules, 2004.
	Technical (if applicable)	Financial (if applicable)		
M/s Digital Arrays	Qualified	Only Technical Qualification was required	Rs.15,176,352/-	Bids of 03 x firms i.e. M/s Digital Arrays, M/s Secure Network, & M/s Tech Avenue were received in tender # NADRA-HQ-RFB-238/2023. The bid of M/s Tech Avenue was disqualified at technical stage for non-complying the compliance sheet. Financial bid of technically qualified firms i.e. M/s Digital Arrays & M/s Secure Network were opened on 15 th February 2024. The bid of M/s Digital Arrays found most advantageous bid.
M/s Secure Network	Qualified	Only Technical Qualification was required	Rs.41,536,000/-	
M/s Tech Avenue	Technically Disqualified			

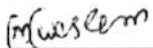
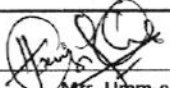


Most Advantageous Bidder: M/s Digital Arrays

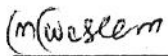
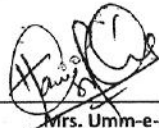
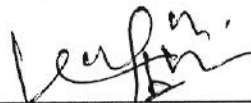

11. Any other additional / supporting information, the procuring agency may like to share. Nil

Signature:

1 n adra 26 2024

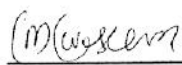
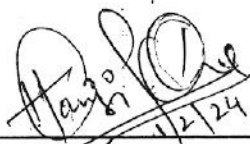



Deputy Director
NADRA HQ Procurement
Imran Hashim
23 February, 2024

		c.	Provider caches conversational threads on dark web/underground forums and marketplaces in full to enable users to understand the complete context of the communication.	The vendor was tasked with presenting communication thread details from dark web sources pertaining to NADRA's assets. However, they were unsuccessful in displaying communication threads, specifically the details of data leakage, for a significant portion of the compromised digital critical information showcased.	Yes	Yes
		d.	Provider offers a flexible range of search operators to perform extensive queries on the data repository and offers the ability to design and implement monitoring rules for near real-time detection of data with proactive alerting to instances of customer proprietary or sensitive data being posted on closed breach databases.	Yes	Yes	Yes
		e.	Provider offers the ability to view the full details of the collected object that triggered said monitoring rule(s). The details will contain the object creation date, the number of replies indicating the length of the thread, the poster of the object, the site from which the object was collected, the original language of the object, the full defanged URL, and the IBAN information (when applicable).	Vendor failed to show the details of all the assets related to NADRA that constitute the NADRA's external attack surface.	Yes	Yes
		f.	Provider offers the ability to integrate the yield of the searches and rule notifications with a comprehensive threat actor profile database.	Yes	Yes	Yes
3	External Attack Surface Management	a.	Provider offers the adversary's view of the complete publicly exposed attack surface with the visibility of all exposed assets of the enterprise.	<ul style="list-style-type: none"> • Vendor failed to show the complete exposed external attack surface. • Active identification of exposed assets could not be demonstrated 	Yes	Yes
		b.	Provider offers information about the vulnerabilities and associated attack vectors corresponding to the exposed assets of the enterprise.	Yes	Yes	Yes
		c.	Provider offers information about the strategies that can be adapted to mitigate the identified vulnerabilities in the exposed assets.	<ul style="list-style-type: none"> • Exclusively recommendations related to the mitigation of vulnerability were not mentioned. • Generic comments were shown during demonstration in the conclusion of reports. 	Yes	Yes
			 Mr. Muhammad Waseem Ali (Deputy Director-IS) President	 Mrs. Umm-e-Hani (Threat Analyst/Scientist-IS) Member	 Mr. Waqas Ali Khan (Deputy Director-T&D) Member	 Mr. Yasir Muhammad Saeed (Deputy Director) Member

		d.	Provider offers realtime continuous monitor of the enterprise's attack surface that can track the progress of any mitigation strategy applied.	Vendor failed to demonstrate the realtime acquisition of monitoring details of all the exposed digital assets. Realtime continuous monitoring is not possible. (Only those assets are being monitored which are added passively to its repository). Vendor failed to show the security gaps related to all the externally exposed digital assets by the perspective of an adversary.	Yes	Yes
		e.	Provider offers realtime information about all security gaps involving publicly exposed assets of the enterprise that includes (but not limited to), injection/RCE vulnerabilities, vulnerable software/libraries used, misconfigured access control, misconfigured encryption, exposed sensitive services or test environments, misconfigured servers, potential DDoS and bypass of CDN service.	Yes	Yes	Yes
4	Multi-Factor Authentication	a.	The proposed solution must incorporate Multi-factor authentication to ensure that access is secure and exclusively granted to authorized users.	Yes	Yes	Yes
5	Period of Subscription / License	a.	The subscription / license of the platform must be of at least 01 year.	Yes	Yes	Yes
6	Support	a.	Support should be available with a guaranteed initial response time.	Yes	Yes	Yes
		b.	On-site initial support for deployment/installation, according to the user requirement, should also be provided.	Yes	Yes	Yes
7	Training (3 X NADRA Officials)	a.	OEM/Principal Certified training for configuration and complete operability of the solution. Training dates can be decided after issuance of purchase order as per convenience of the user-department.	Yes	Yes	Yes
		b.	The vendor should also provide a list of electronic and printed documentation for the installation, operation, use, and administration of the entire solution.	Yes	Yes	Yes
8	Qualification Status			Disqualifies	Qualifies	Qualifies
<div style="display: flex; justify-content: space-between; align-items: flex-end;"> <div style="text-align: center;">  <hr/> Mr. Muhammad Waseem Ali (Deputy Director-IS) President </div> <div style="text-align: center;">  <hr/> Mrs. Umm-e-Hani (Threat Analyst/Scientist-IS) Member </div> <div style="text-align: center;">  <hr/> Mr. Waqas Ali Khan (Deputy Director-T&D) Member </div> <div style="text-align: center;">  <hr/> Mr. Yasir Muhammad Saeed (Deputy Director) Member </div> </div>						

2024

Technical Evaluation of CTI Platform (Tender# NADRA-HQ-RFB-238/2023)				
S#	Feature	M/s Tech Avenue	M/s Digital Arrays	M/s Secure Network
1	Past Relevant Experience of minimum 2 years of Similar Nature	Yes	Yes	Yes
2	Audited Bank Statement of last 2 years	Yes	Yes	Yes
3	Bidder must be authorized partner of OEM and certificate must be submitted	Yes	Yes	Yes

 Mr. Muhammad Waseem Ali (Deputy Director-IS Department) President	 Mrs. Umm-e-Hani (Threat Analyst/Scientist-IS Department) Member 1
 Mr. Waqas Ali Khan (Deputy Director-Technology Department) Member 2	 Mr. Yasir Muhammad Saeed (Deputy Director-Network Department) Member 3