पुलिस मुख्यालय राजस्थान जयपुर
परिशिष्ट–ई

Specification for Open Source Intelligence Gathering Software:- क्रय हेतु शर्ते एवं स्पेसिफिकेशन
सामान्य शर्तो से संबधित परिशिष्ट ''स'' में कम् सं. 1 से 31 तक अंकित शर्तो के अलावा निम्न शर्ते एवं विवरण लागू होगे ।

Specification for Open Source Intelligence Gathering Software:- के सम्बन्ध में एफ. ओ.आर.मात्रा, स्पेसिफिकेशन का विवरण निम्नानुसार है:–

(क) एफ.ओ.आर.:– केन्द्रीय भण्डार, पुलिस मुख्यालय, राजस्थान, जयपुर
(ख) मात्रा          —  01 Nos.
(ग) सप्लाई अवधि   – 30 दिवस
(घ) स्पेसिफिकेशन

Open Source Intelligence Gathering Software

| Sr. No. | Technical Requirements | Compliance Yes/No |
|---|---|---|
| 1. | The platform must be designed for the goals of information collection, making prompt managerial decisions, controlling and monitoring objects of several types, situations, and other functions. | |
| 2. | The main tasks solved by the system must include background and contractor checks, information security incident analysis, investigating economic crimes, monitoring the social and political situation in the information space, and supporting operational search activities. | |
| 3. | The platform must be designed for use by analysts among the staff of law enforcement agencies, government and special services, corporate and cybersecurity specialists, private detectives, etc. | |
| 4. | The platform must be built via SaaS principles and allow user unimpaired access to the system over the network from any personal computer without the need to install any additional software except network browser. | |
| 5. | The platform should use project-based organization of the user workflow (so a user could create a project, perform an investigation and save the results within it, share or delete this project) and project grouping capability so that the information from a project could be accessed from other projects within its group. | |
| 6. | The platform data model must be ontological in nature allowing users to create, change or use any of existing hierarchically structured data types (e.g. a person, a company, a vehicle, etc.) | |
| 7. | The platform must support language packages and provide users the ability to change user interface language. | |

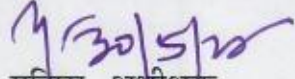| | | |
|---|---|---|
| 8. | The platform must automate the investigation cycle including its initialisation, input, gather, analysis, and report phases as described below | |
| 9. | The platform must include an access control mechanism as the basis for its users' registration, authentication, and authorization | |
| 10. | The platform must allow manual user data input as well as import functionality including text (txt, doc), image (jpg, png), table (xls, xlsx) and map (kml, kmz) file import | |
| 11. | The platform must provide users the capability of information gathering from the following sources: Facebook, Foursquare, Instagram, LinkedIn, Myspace, TikTok, Twitter, VK, Xing, Skype , Snapchat , Telegram , WhatsApp, Tumblr, Tinder, Steam, Google, Gravatar, Yandex Images, Companies House, OCCRP, Offshore Leaks, Open Corporates, Sanctions Explorer, Bit query, Wikileaks, , DocumentCloud, Flickr, Vulners. | |
| 12. | The platform must provide users the capability of data visualization in the following forms: Graph view, Table view, Map view, Text view, Image view. Each view must allow users to interact with the data in the following ways: View information, Add information (manually and automatically in the Gather phase), Use information as input to the data collection algorithms (in the Gather phase), Edit information (delete, append or change in the Analysis phase). | |
| 13. | The platform must provide the following data processing functionality: Search and filtering within the project, Timeline visualization for the timestamped objects and connections, Automated machine-learning algorithms such as Natural language processing (named entity recognition, sentiment analysis, translation, hate speech detection, etc.), Computer vision (facial detection and recognition, object detection (cars, guns, etc.), etc.). | |
| 14. | The proposed solution must provide the following automation functionality: Task manager functionality (displaying all running tasks within the project, capability to restart or stop them and view results for each task). Automated gathering and data processing methods run via script automation (with the possibility to create scripts with a no-code visual editor), Delayed, scheduled and periodical gathering and data processing methods run via monitoring functionality (with the possibility to compare results and alert users on their change). | |
| 15. | The Platform must have a built-in presentation mode with an autoplay function as well as a report building and export functionality. | |

| 16. | The Platform should search and provide Structured and parsed data leaks. Personal data and account details involved in the breaches. Needed for finding connections between phone numbers, social media accounts, crypto wallets, and email addresses. Contains: Names and usernames, Passwords, IP addresses, Emails and email domains used, Crypto wallets, Phone numbers, Social media (Facebook, Instagram, etc.) accounts, 240 billion processed attributes, 165 million processed identity breach records, 165 thousand of analysed breaches, 15 years of breaches. | |
|---|---|---|
| 17. | The Platform should search and provide Structured data stolen from laptops via malware and posted on the Dark Web (device "snapshot"). Contains: Device browser history, Names and usernames, Passwords, Device serial numbers, Emails and email domains used, Crypto wallets, Phone numbers. | |
| 18. | The Platform should search and provide Data from darknet marketplaces and forums, paste sites, and alternative social media. Needed for analysing threads and discussions on forums and identifying the authors, viewing marketplace listings, and investigating vendors.<br>Contains: Names and usernames, Comments & threads on forums, Crypto wallets, Emails, and email domains used, Phone numbers, Vendors from marketplaces and products they sell . | |
| 19. | The Platform should have minimum 2 years Subscription License for Single User | |

सामान्य शर्तें:-

1. उल्लेखित उपकरणों का डैमोस्ट्रेशन/प्रैजेन्टेशन बोली खुलने के तीन दिवस में करने के निर्देश दिये जा सकते है। जिसकी पालना फर्म द्वारा आवश्यक रूप से करनी होगी।

2. उपरोक्त आईटम की गारन्टी/वारन्टी 2 वर्ष एवं उपकरण का सॉफ्टवेयर अपडेट व सर्विस सपोर्ट 2 वर्ष की अवधि तक होगी।

3. बोली में दर्शित प्रत्येक वस्तु की दर मय एक्सैसरीज के स्पेसिफिकेशन के अनुसार अंकित की जावें ।

4. विभागीय स्पेसिफिकेशन के अनुसार बोली सूचना एवं परिशिष्ट में अंकित प्रत्येक आईटम की पूर्ण मात्रा हेतु दर दी जावें तथा दर प्रति नग दी जावे। यदि किसी बोलीदाता द्वारा समान स्पेसिफिकेशन हेतु एक से अधिक दर दी जाती है तो बोली के उद्देश्य से न्यूनतम दर को गणना में लिया जावेगा।

5. उपकरण/वस्तु के सम्बन्ध में तकनीकी विवरण से सम्बन्धित पूर्ण दस्तावेज स्कैन करके ई-बोली के साथ दिये जावे।

6. सप्लाई के समय माल का निरीक्षण विभागीय निरीक्षण समिति या अतिरिक्त महानिदेशक पुलिस, आयोजना, आधुनिकीकरण एवं कल्याण, राजस्थान जयपुर द्वारा मनोनीत प्रतिनिधि या कमेटी द्वारा किया जावेगा ।

7. निरीक्षण प्रभार यदि कोई हो तो आरम्भ में सप्लायर द्वारा निरीक्षणकर्ता को दिया जाएगा तथा यदि निरीक्षण में माल सही पाया गया तो निरीक्षण प्रभार का पुर्नभरण विभाग द्वारा सप्लायर को कर दिया जावेगा। यदि माल सही नहीं पाया गया तो निरीक्षण प्रभार विभाग द्वारा देय नहीं होगा।

8. निर्माता कम्पनी के राज्य में उपलब्ध सर्विस केन्द्रों की सूची स्कैन करके बोली के साथ प्रस्तुत करे।

9. सप्लायर द्वारा परिशिष्ठ ई की शर्तों अनुरूप उपकरण का Instalation करना होगा।
10. सप्लायर को विभाग द्वारा मनोनीत किये गये कार्मिकों को निःशुल्क प्रशिक्षण उपलब्ध करवाना होगा।

पुलिस अधीक्षक,
केन्द्रीय भण्डार, पुलिस मुख्यालय,
राजस्थान, जयपुर ।

मैंने/हमनें उपरोक्त समस्त शर्तों की ध्यानपूर्वक पढ़कर अच्छी तरह समझ लिया है तथा समस्त शर्तों के पालन हेतु सहमत हूँ/है ।

हस्ताक्षर बोलीदाता मय मोहर
बोली की समस्त शर्तें स्वीकार करने के प्रमाण रूप मे