

Commercial Confidential

Appendix 3 List of Requirements

attached to the Descriptive Document

Status : version 1.0

Reference : TN/489170

INTRODUCTION

The Proposal must meet minimum requirements. If Contractor does not meet these requirements, Client will not include the Proposal in the assessment. Requirements are therefore minimum preconditions that the Proposal must meet in order to be assessed. Client describes the requirements below.

The requirements are divided into 7 categories. Each category has its own table. Every requirement has a description in the same row. In the same row is also set out whether the requirement applies to one of the lots or to both lots. An X in column L1 indicates it applies to Lot 1 and an X in column 2 indicates it applies to Lot 2. For instance, Requirement 1.1 applies to both lots, since column L1 and L2 are marked with an X and Requirement 2.1 only applies to Lot 2 since only column L2 is marked with an X. The last column indicates which of the MoSCoW-criteria apply. Must have [MUST] indicate the Proposal needs to meet the requirement in full. Failing to meet a requirement indicated as Must results in a knockout and will not be assessed by the Assessment Team. Should have do not necessarily need to be met, but if the requirement is met, up to 20 points can be awarded for meeting the requirement. Could have also do not necessarily need to be met, but if the requirement is met, up to 10 points can be awarded for meeting the requirement.

If Tenderer conforms that they comply with a SHOULD or COULD requirement, this needs to be clarified in Appendix 5A for Lot 1 and/or 5B for Lot 2. If Tenderer does not explain how SHOULD or COULD-requirements are met, Tenderer will not receive any points for the particular requirement.

1. GENERAL REQUIREMENTS

ID	Description	L1 (Feed)	L2 (Dash-board)	MoSCoW
1.1.	Contractor declares that, in drawing up its Tender, it has taken account of the obligations that apply in respect of Dutch and European legislation and regulations and indemnifies Client against any liability regarding non-compliance with the obligations arising from this.	X	X	MUST
1.2.	Contractor monitors the developments in laws and regulations relevant to Client and advises on these in the context for Client. It is necessary to draw Client's attention in good time to (possible) changes in laws and regulations and the (possible) impact of these for Client.	X	X	MUST
1.3.	Contractor shall act in accordance with the application code of the Dutch Association for Personnel Management & Organization Development (NVP), as described at: https://www.nvp-hrnetwerk.nl/sollicitatiecode .	X	X	MUST
1.4.	The offered system includes all requirements (MUST, SHOULD and COULD) as stated by Contractor when filling the provided forms. The offered system (including interfaces) is readily available and available as a standard application offered by Contractor at the time Contractor's offer/quotation is issued to Client.	X	X	MUST

1.5.	Contractor is competent, has and maintains knowledge of developments in the Cyber Security domain and, based on this, is able to provide, implement and maintain an integrated system for Client and its chain partners.	X	X	MUST
1.6.	Contractor agrees to the ARIV terms of delivery.	X	X	MUST
1.7.	Contractor agrees to the preconditions of execution mentioned in the tender documents.	X	X	MUST
1.8.	Contractor warrants that its offer covers the entire desired situation/mission and that upon award, Contractor will deliver a working solution in accordance with the requirements in the tender documents and make every effort to implement it correctly and in a timely manner.	X	X	MUST
1.9.	The system's online help facility is updated for timeliness and regulatory requirements by Contractor with each new release.	X	X	MUST
1.10.	At a minimum, the system should support the use of diacritics as required by law.	X	X	MUST

2. FUNCTIONAL REQUIREMENTS

ID	Description	L1 (Feed)	L2 (Dash board)	MoSCoW
2.1.	Ability to collect and process threat intelligence data from multiple sources, including open-source feeds, industry-specific sources, and commercial threat intelligence providers.		X	MUST
2.2.	Ability to provide insights into current and relevant threat intelligence for the Dutch healthcare sector, at the strategic and tactical level.		X	MUST
2.3.	Ability to provide insights into current and relevant threat intelligence for the Dutch healthcare sector, at the operational and technical level.	X		MUST
2.4.	Ability to integrate with multiple news sources through APIs or web scraping to collect and aggregate news articles in real-time.		X	MUST
2.5.	Ability to integrate with third-party tools and services, such as analytics and reporting tools.		X	MUST
2.6.	Ability to generate and export reports, metrics and diagrams covering a predefined period (week, month, quarter, year) for healthcare in Europe, in the world or a specific country.		X	MUST
2.7.	Ability to share the results of analysts' investigations with the constituency of Client member and partner organizations.	X	X	MUST
2.8.	The threat intelligence must cover the entire cyber domain, including information on geopolitical developments.		X	SHOULD
2.9.	Relevant threat intelligence must include: Insight into sector-specific threats, techniques, tactics, and procedures (TTPs) used by threat actors, malicious software (malware), including indicators of compromise (IOCs), threats in the supply chain, threats to suppliers,	X	X	SHOULD

	information about vulnerabilities in IT products, and exposure of confidential information from or about members of Client on the dark web, including insight into data breaches of healthcare entities.			
2.10.	Ability to monitor data leak websites of Ransomware-as-a-Service (RaaS) actors for any mention of Dutch healthcare organizations or their supply chain. Ability to analyze this dataset. For example: generate a chart of all ransomware/extorting incidents on data leak websites.		X	SHOULD
2.11.	Ability to monitor hacktivist groups communication channels for any mention of Dutch healthcare organizations or their healthcare supply chain. Ability to analyze this dataset. For example: generate a chart of all DDoS attacks on healthcare.		X	SHOULD
2.12.	Ability to monitor dark web for any mentions of Dutch healthcare organizations or their supply chain. For example: access to a network of a Dutch healthcare organization is sold.		X	SHOULD
2.13.	Ability to identify and prioritize the most relevant threats based on impact, probability, and other factors.	X	X	SHOULD
2.14.	Ability to search and filter threat intelligence data based on various criteria, such as date, topic, and source.	X	X	SHOULD
2.15.	Ability to provide real-time updates and notifications to users through push notifications or email alerts.	X	X	SHOULD
2.16.	Support for parsing information in multiple languages, such as Dutch and other non-English languages.		X	SHOULD
2.17.	Customizable dashboards and visualizations to display threat intelligence data in a meaningful way.		X	COULD
2.18.	Ability to create alerts and notifications for Client based on predefined rules and thresholds.	X	X	COULD
2.19.	Ability to display news articles in a user-friendly and visually appealing way, using summaries and headlines.		X	COULD
2.20.	Customizable dashboard and layout to allow users to personalize their news feed and display preferences and share these with others.		X	COULD
2.21.	Ability to display trending topics and related news articles to keep users informed of current events.	X	X	COULD
2.22.	Ability to save articles for future reference or offline reading.		X	COULD
2.23.	Integration with third-party news sources to provide a comprehensive and diverse news feed.		X	COULD
2.24.	Ability to support different user roles and permissions to ensure appropriate access and control of the news feed.		X	COULD

3. TECHNICAL REQUIREMENTS

ID	Description	L1 (Feed)	L2 (Dash- board)	MoSCoW
3.1.	Support for standard threat intelligence formats including STIX/TAXII and MISP.	X	X	MUST

3.2.	Ability to integrate with third-party threat intelligence providers and feeds.	X	X	MUST
3.3.	Compatibility with industry-standard security protocols including SSL/TLS and SAML.	X	X	MUST
3.4.	Support for secure communication protocols including SSL/TLS to protect user data and privacy.	X	X	MUST
3.5.	Ability to exchange data with other software systems through APIs or other integration methods (API consumer). Documentation about these integration options is provided.	X	X	MUST
3.6.	Solution provides well documented APIs for automated access to its core functionalities (API provider). These API's are built on industry standard technology.	X	X	MUST
3.7.	Support for industry-standard data exchange formats, including CSV, JSON and XML.	X	X	MUST
3.8.	The solution is a cloud-based Software-as-a-Service (SaaS) solution.	X	X	MUST
3.9.	Contractor provides clear insight in which functions and APIs support which Lot of this procurement, so Client can assess how interwoven both functionalities are.	X	X	MUST
3.10.	Supplier provides a test and a production environment without any additional charges. The test environment can work with fictional data.	X	X	MUST
3.11.	The solution is accessible over the internet, using IPv4 or IPv6.	X	X	MUST
3.12.	Provided APIs adhere to the ' NLGov REST API Design Rules 2.0.0' (https://gitdocumentatie.logius.nl/publicatie/api/adr/) and Open API Specification (OAS) version 3.0 (https://swagger.io/specification/). In the event Contractor cannot meet these requirements, API's are at least described in the form of REST/JSON.	X	X	SHOULD
3.13.	Ability to process large amounts of unstructured data, such as social media feeds and dark web forums.		X	SHOULD
3.14.	Ability to process and analyze large volumes of news articles in near real-time.		X	SHOULD
3.15.	Compatibility with different operating systems, including (Windows, MAC, Linux) and web browsers (Chrome, Edge, Firefox, Safari).	X	X	SHOULD
3.16.	Responsiveness and fast loading times to provide a seamless user experience.	X	X	SHOULD

4. PRIVACY REQUIREMENTS

ID	Description	L1 (Feed)	L2 (Dash-board)	MoSCoW
4.1.	Contractor must follow the main principles mentioned in the Algemene verordening persoonsgegevens (AVG) (General Data Protection Regulation (GDPR)) in which these principles are contained such as privacy by design and default. This policy must allow	X	X	MUST

	Client to fulfill its own obligations under the GDPR. The purpose of processing personal data must be determined, such as storing personal data within an application to build a personnel file, or a CRM system to store and consult participant data.			
4.2.	Contractor must have a legal basis for processing personal data under the AVG (GDPR).	X	X	MUST
4.3.	Contractor must have a retention period concerning the processing of personal data, and it must store the minimum necessary personal data to achieve the intended purpose.	X	X	MUST
4.4.	Contractor must ensure the accuracy and correctness of personal data being processed by the software tool.	X	X	MUST
4.5.	Contractor must adequately secure (special) personal data.	X	X	MUST
4.6.	Contractor must inform all data subjects involved, such as Client's employees, contact persons, participants, and any other stakeholders, of the intended processing and meet the information obligation that rests on Client.	X	X	MUST
4.7.	If required, Contractor must conduct a mandatory DPIA, as per the list provided by the Dutch Data Protection Authority (Autoriteit Persoonsgegevens).	X	X	MUST
4.8.	The privacy statement of Contractor must not show that personal data being processed outside the European Economic Area (EEA). If personal data is processed outside the EEA, Contractor must provide sufficient safeguards, such as Binding Corporate Rules (BCR), Code of Conduct, or Model Contracts, and consult the Privacy Officer of Client to ensure GDPR compliance.	X	X	MUST
4.9.	If applicable, Contractor must comply with the adequacy decision by the European Commission, if any, indicating that the country where the personal data is processed complies with the GDPR.	X	X	MUST
4.9.	If applicable, Contractor must comply with specific exceptions, as per Art. 49 GDPR in the event that the requirements of 4.9 and/or 4.10 are not met.	X	X	MUST
4.10.	In accordance with the GDPR, Client and Contractor must enter into a Data Processing Agreement, if during the process the role of the supplier is that of a processor under the GDPR.	X	X	MUST
4.11.	If applicable, Contractor does not make use of sub processors without notifying and the written authorization of Client.	X	X	MUST
4.12.	In the case of a personal data breach Contractor has a clear process in notifying Client if the breach involves personal data for which Client acts as a controller.	X	X	MUST
4.13.	Contractor makes it possible for data subjects to exercise their rights under the GDPR, such as the right to rectification, erasure, restriction and data portability of personal data.	X	X	MUST
4.14.	If applicable, Contractor does not make use of any form of automated individual decision-making, including profiling of data subjects.	X	X	MUST
4.15.	If applicable, Contractor does not make use of AI without consent of Client and information about the consequences for the processing of personal data for which Client is data controller. Personal data is not used to train Contractor's own large language model (LLM) if applicable.	X	X	MUST

4.16.	If applicable the software tool should have a function to turn off AI (by default) in accordance with the privacy policy of Client.	X	X	SHOULD
-------	---	---	---	--------

5. SECURITY REQUIREMENTS

ID	Description	L1 (Feed)	L2 (Dash- board)	MoSCoW
5.1.	The software tool must use secure connections, with a minimum TLS 1.2.	X	X	MUST
5.2.	The software tool must always provide a valid certificate that is trusted by all current major web browsers (Chrome, Edge, Firefox, Safari).	X	X	MUST
5.3.	The software tool's user and configuration data is backed up by provider to prevent data loss. Contractor carries out regular restore tests to verify that the data can be restored (minimally once a year). It must be possible to restore Client's user and configuration data at the request of Client, independent from other customers.	X	X	MUST
5.4.	The software tool's data is exportable by users in a usable format (either by using open standards or by providing proper documentation).	X	X	MUST
5.5.	The software tool must encrypt our data at rest and in transit (both internally and externally) to prevent data breaches, unauthorized access or disclosure (accidental and/or intentional).	X	X	MUST
5.6.	The software tool must provide authentication with MFA.	X	X	MUST
5.7.	The software tool must log authentication attempts and these logs must be visible to us.	X	X	MUST
5.8.	The software tool must time out after five login attempts wherever possible.	X	X	MUST
5.9.	The software tool must have audit logging (which includes times, usernames, performed actions), which is available to us.	X	X	MUST
5.10.	Contractor performs periodic vulnerability scanning (runtime and/or code) to identify vulnerabilities.	X	X	MUST
5.11.	The software tool is actively maintained and developed to ensure its security and the use of current technology with continuously improving features.	X	X	MUST
5.12.	Available patches for critical vulnerabilities (with a CVSS v3.x rating > 8.9) will be applied by Contractor within 2 calendar days. This includes the patching or subcomponents and dependencies.	X	X	MUST
5.13.	The software tool supports assigning roles and authorizations to users (Role Based Access Control).	X	X	MUST
5.14.	The Service Level Agreement guarantees system availability of 99,8% on a yearly basis. Scheduled outages are calculated as unavailability. Documentation is available to demonstrate measures to meet this goal.	X	X	MUST

5.15.	Client will be informed by Contractor in advance on the plan, communicate and execute scheduled outages and informed on the expected time windows.	X	X	MUST
5.16.	The software tool is protected against data corruption or loss. Documentation of measures is supplied.	X	X	MUST
5.17.	Client retains legal ownership of its data and user input.	X	X	MUST
5.18.	Contractor has a valid ISO 27001 certification, or equivalent, and supplies the certificate including statement of applicability that fully covers the solution offered. Supplier ensures that subcontractors are also ISO 27001 certified, or equivalent, for the services that are relevant to the software tool and related services offered to Client. In the absence of an ISO 27001 certification, Contractor and/or its subcontractors are obligated to prove/demonstrate the equivalent is up to the standards of an ISO 27001 certification.	X	X	MUST
5.19.	The data of Client is logically separated from other customers' data at rest.	X	X	MUST
5.20.	Contractor ensures that all subcontractors adhere to at least the same level of security controls, restrictions and considerations that apply to Contractor.	X	X	MUST
5.21.	Contractor notifies Client of security incidents regarding Client's data as soon as possible, but no later than 48 hours.	X	X	MUST
5.22.	Outbound email sent by Contractor and the software tool on behalf of Client is protected from spoofing and misuse by SPF, DKIM, DMARC and STARTTLS with DANE.	X	X	MUST
5.23.	The software tool should use SSO with Client's Entra ID.	X	X	SHOULD
5.24.	In case SSO with Entra ID is offered, MFA should be possible for users that are not authenticated through Entra ID (e.g. for emergency access accounts to be used in case SSO is not available).	X	X	SHOULD
5.25.	Contractor monitors systems that store or process our data for availability and security purposes.	X	X	SHOULD
5.26.	Contractor is willing to include a right to audit in the agreement.	X	X	SHOULD
5.27.	The data of Client is physically separated from other customers' data at rest.	X	X	SHOULD
5.28.	The data of Client is not accessible by Contractor's employees (e.g. support staff) without prior approval by Client. Both technical and organizational measures to prevent access are in place and enforced by Contractor.	X	X	SHOULD
5.29.	Contractor provides contact options and the associated response times and/or service levels to Client.	X	X	SHOULD
5.30.	Contractor assists with security investigations and legal discovery.	X	X	SHOULD
5.31.	Contractor fully compensates Client in case of a security breach that is caused by Contractor or its subcontractors.	X	X	SHOULD
5.32.	DNS records used by the software tool and services provided to Client by Contractor are protected by DNSSEC.	X	X	SHOULD
5.33.	The software tool's logging can be ingested by our security incident and event management solution (SIEM).		X	SHOULD
5.34.	The software tool's logging can be ingested by our security incident and event management solution (SIEM).	X		COULD
5.35.	The software tool could log authorization mutations and attempts to break them.	X	X	COULD

5.36.	In case of an emergency, Contractor can be contacted and provides support 24/7 for a suspected security breach or incident, based on Client's judgement that it has (potentially) very high impact.	X	X	COULD
-------	---	---	---	-------

6. ADMINISTRATION AND INVOICE REQUIREMENTS

ID	Description	L1 (Feed)	L2 (Dashboard)	MoSCoW
6.1.	The licenses provided by Contractor will be approved annually by Client.	X	X	MUST
6.2	Invoicing takes place annually in December for the number of agreed licenses for the coming twelve (12) months.	X	X	MUST
6.3	Client will only process invoices if they are sent with the correct invoice numbers and other invoice details. After the award is final, this information will be provided by Client.	X	X	MUST
6.4	The method of invoicing may be subject to change. In the event the method of invoicing is changed, Contractor will cooperate in consultation with Client.	X	X	MUST

7. COMMUNICATION REQUIREMENTS

ID	Description	L1 (Feed)	L2 (Dashboard)	MoSCoW
7.1.	During the contract period, communication, either verbally or in writing, will be in the Dutch or English language.	X	X	MUST
7.2.	Contractor shall appoint one central point of contact (account manager) and one permanent replacement for all communications related to the execution of the Framework Agreement.	X	X	MUST
7.3.	The account manager (and permanent substitute) shall have knowledge of the content of the Framework Agreement, be available on working days between 8:00 a.m. and 6:00 p.m., Central European Time (CET), by mail and telephone, act in a problem-solving manner, and contact Client within one (1) working day in the event of a question or desired point of contact.	X	X	MUST
7.4.	In the event of replacement/succession of the permanent contact person, Client shall be informed no later than one (1) month prior to the replacement/succession. In case of temporary absence of the permanent contact person, a replacement must be appointed at all times who is familiar with Client and the contents of the Framework Agreement. Client reserves the right to request a replacement contact person if, in the opinion of Client, the cooperation is not going as desired.	X	X	MUST

7.5.	Contractor is capable of providing the services described in the Descriptive Document (including appendices) at unchanged quality throughout the term of the Framework Agreement.	X	X	MUST
7.6.	Contractor shall inform Client as soon as Contractor becomes aware that fulfillment of the Assignment cannot take place or cannot take place on time or properly. Notification will take place immediately by email and telephone, stating the underlying reason(s).	X	X	MUST
7.7.	Consultations will be held at the operational level if it appears that the services are not being performed in accordance with the Schedule of Requirements. Operational consultation can take place within five (5) working days.	X	X	MUST
7.8.	Agreements shall be recorded in writing by Contractor. Both parties shall have a copy of these records.	X	X	MUST
7.9.	In the event of early termination or dissolution of the Framework Agreement, Contractor must guarantee an effective and smooth transfer of work and information to any new party. All updated data in Contractor's possession relating to the Framework Agreement will be made available to Client digitally on demand.	X	X	MUST
7.10.	A helpdesk shall be responsible for handling all notifications and incidents related to the system according to the Service Level Agreement (SLA) procedure. The priority of incidents shall be determined by Client in consultation with the service provider.	X	X	MUST
7.11.	The following priority classification should be used by the helpdesk: 1. Critical: The system is completely unavailable 2. Major: The system is partially unavailable 3. Minor: Minor disruptions 4. User / administrator inquiry The helpdesk shall also be responsible for relating incidents to known system problems. Contractor shall inform Client of the incident handling status. Contractor shall be responsible for incident management. The response time for incidents shall be as follows: 1. Response: < 30 minutes; Solution or Workaround: < 4 hours 2. Response: < 1 hour (during office hours); Solution or Workaround: < 8 hours 3. Response: < 24 hours; Solution or Workaround: < 72 hours 4. Response: < 1 week For workarounds, a definitive solution shall be provided in the next regular version.	X	X	SHOULD