



Appendix A

DRAFT Schedule of Requirements

Market Consultation

*Continuous Phishing and Phishing
Incident Response*

Table of contents

1. General requirements	2
2. Phishing Incident Response	2
2.1 Assessments	2
2.2 Integration	2
2.3 Reporting process	2
3. Security reporting & Performance insights	3
3.1 Reporting Security reporting & Performance insights	3
4. Phishing simulation & Security training	3
4.1 Reporting Phishing simulation & Security training	3
4.2 Campaign management	3
4.3 Onboarding	4
4.4 Engagement	4

DRAFT

1. General requirements

Nr.	Requirements regarding general requirements
1.1	The training application in the Tool does not negatively affect the ability to report or the clarity of the process for reporting a suspicious message.
1.2	The Contractor must offer at least Dutch and English as working languages.

2. Phishing Incident Response

2.1 Assessments

Nr.	Requirements regarding assessments
2.1.1	Emails/campaigns already assessed by Enexis (benign or malicious) must be handled automatically.
2.1.2	The Tool automatically provides an initial assessment of an email's safety, based on up-to-date information about campaigns, threats, and technological developments.
2.1.3	The Tool offers the ability to filter reported emails based on adjustable conditions to determine when analysis and mitigation are required. Possible filtering criteria include, at a minimum: • The outcome of the automatic provisional assessment • The Tool provides feedback to reporters after assessment. For each report, a manual comment can be added to the response.

2.2 Integration

Nr.	Requirements regarding integration
2.2.1	Integration with Microsoft Defender/Sentinel (including support for parsing evidence) or ServiceNow Security Incident Response (including support for parsing observables) is required to enable follow-up by analysts via a single pane of glass and for reporting purposes.
2.2.2	The Tool must support the purging of malicious emails directly from within the solution.
2.2.3	Suspicious emails must be reportable from any type of mailbox (personal, shared/functional) and from any type of Outlook client, in a user-friendly manner without technical limitations.
2.2.4	The Tool must enable data exchange via an API or a comparable standardized interface to ensure seamless integration for authentication and user (de)provisioning, supporting existing protocols such as SCIMv2, OIDC, OAuth2, and SAML.

2.3 Reporting process

Nr.	Requirements regarding reporting process
2.3.1	The Contractor must link Microsoft's standard reporting process to the reporting of unwanted and suspicious emails. The Contractor is also required to report to Microsoft (forwarding to Microsoft).
2.3.2	The Tool must provide feedback to reporters after an email has been assessed. For each report, a manual comment can be added to the response.
2.3.3	Any email communications (such as feedback on a report) must be sent on behalf of the Enexis.nl domain and must follow the Enexis corporate branding guidelines.
2.3.4	The Contractor must offer the ability to edit text within user interfaces as part of the reporting process.
2.3.5	The Tool must support tracing emails via Microsoft Exchange/Defender MS365 that are part of the same threat campaign.
2.3.6	Reports concerning simulation emails must not be processed through the regular phishing response workflow.

3. Security reporting & Performance insights

3.1 Reporting Security reporting & Performance insights

Nr.	Requirements regarding Reporting Security reporting & Performance insights
3.1.1	The Contractor must continuously provide insights through a reporting dashboard, with download/export capability. Data that must be reported: • number of reports per team • type (simulation or real email) • threat categories and tactics • assessment (final classification).
3.1.2	The Contractor must provide the ability to show insight into the successful delivery of simulation emails, including whether the email has been read.
3.1.3	Reporting must be possible at both individual level and aggregated by department and organizational unit.
3.1.4	Enexis must be able to download a printout of the real-time data at any time.
3.1.5	The Contractor must share a general message with users when multiple phishing emails are received by multiple users, to raise awareness about the phishing email.
3.1.6	The Contractor must continuously enrich the offering of simulation emails based on current threats (such as trends and those arising from technological innovations and current events).
3.1.7	Single Sign-On must be used to access the reports (dashboard).
3.1.8	Involved employees must be able to consult personal information about their results (score) via the dashboard.
3.1.9	Involved employees must gain insight into the status of reported actual phishing emails.
3.1.10	Designated administrators must have access to individual scores at an aggregated level (dashboards).

4. Phishing simulation & Security training

4.1 Reporting Phishing simulation & Security training

Nr.	Requirements regarding reporting phishing simulation & security training
4.1.1	Users must have access to their own performance regarding simulated phishing emails.
4.1.2	The Tool must train and measure at least the following aspects of a user's response to a simulated email: • Message replied to • Attachment opened • Hyperlink clicked • Credentials entered on the landing page, file downloaded, permissions granted, clickfix script executed • Credentials entered in the attachment, script allowed/permissions granted.

4.2 Campaign management

Nr.	Requirements regarding campaign management
4.2.1	The Contractor must provide the ability to use previous real phishing emails received by Enexis as a training opportunity.
4.2.2	The Contractor must provide the option for the client to initiate a simulation campaign themselves, targeting specific groups.
4.2.3	The Contractor must offer an adaptive difficulty level that is tailored to the individual level and any potential learning path of the user.

4.2.4	The Contractor must provide the option for Enexis to create its own simulated phishing email.
4.2.5	The continuous phishing service is fully managed by the provider, with the requester periodically involved (preferably monthly) for further coordination.
4.2.6	It must be possible to test specific target groups based on departments, roles, location, and risk profile.
4.2.7	It must be possible to test organization-wide in a single run.
4.2.8	It must be possible to send the phishing email entirely in Enexis corporate style.
4.2.9	It must be possible to fully or partially customize the landing page shown after clicking a link in a phishing email, based on Enexis's instructions (fully in Enexis corporate style).
4.2.10	If a login page is used during the phishing activity, it must reflect the corporate style of the requested login page.
4.2.11	The requester must be able to propose a specific topic or content for a phishing campaign.
4.2.12	Phishing simulations must be able to include images (such as QR codes).
4.2.13	The Tool must have a WYSIWYG editor and HTML editing capabilities for simulation emails and landing pages.
4.2.14	The Contractor must offer the possibility to provide alternative phishing options (at minimum: deepfake and Teams).

4.3 Onboarding

Nr.	Requirements regarding onboarding
4.1.1	Employees must be automatically added upon onboarding and removed upon offboarding.
4.1.2	New employees must receive onboarding material via the Tool.

4.4 Engagement

Nr.	Requirements regarding engagement
4.4.1	The Contractor must provide the option to offer interactive game formats to increase engagement.