ENEXIS PERSONEEL B.V.

Appendix 02.1

Schedule of Requirements

Continuous phishing and Phishing incident response

Table of contents

1. Introduction

This document sets out the requirements that the Contractor must comply with throughout the term of the Agreement. The requirements in this document concern functional requirements. The non-functional requirements are included in *Appendix 02.2 - Schedule of Non-functional Requirements*.

For each requirement, it is indicated whether it relates to Continuous phishing tooling, with the abbreviation CP, or to Phishing incident response tooling, with the abbreviation PIR. If the requirement applies to both tools or to the service in general, then nothing is indicated for that requirement.

Enexis aims, for Phishing incident response, to integrate with messaging, security and incident response products already in use by Enexis, being Microsoft 365 and Exchange, Microsoft Sentinel and Defender for MS365 and ServiceNow Security Incident Response. For the PIR tool requirements set out below, its capabilities may be used as part of the proposed solution, provided that this meets the functional requirement.

1.1 General requirements

Nr.	Requirements regarding general requirements
1.1.1	End users follow the same reporting process for both simulated and real threats, without any distinction.
1.1.2	All interfaces and training content must be made fully available to end users in both English and Dutch.
1.1.3	Contractor engages only those (sub)contractors that are established, registered, and operational in a country that has signed the Government Procurement Agreement (GPA).
1.1.4	The Contractor allows for role-based access control for various data and insights.

1.2 Onboarding & offboarding

Nr.	Requirements regarding onboarding & offboarding
1.2.1	New employees must receive onboarding material.
CP1.2.2	The Contractor must provide a functionality that automatically sends periodic notifications to new employees who do not participate in mandatory phishing simulations. Notifications should be adjustable by Enexis.
CP1.2.3	Enexis must be able to pause simulations for individual End users.

2. Phishing incident response (PIR)

2.1 Assessments

Nr.	Requirements regarding assessments
PIR2.1.1	For phishing events/campaigns already assessed by Enexis (benign or malicious), the same classification is applied automatically and the report is processed accordingly.
PIR2.1.2	The PIR tooling automatically provides an initial assessment of a message's safety, based on up-to-date information about campaigns, threats, and technological developments.
PIR2.1.3	The PIR tooling offers the ability to filter reported messages 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 • message directionality • contains URLs • contains attachments.

2.2 Integration

Nr.	Requirements regarding integration
PIR2.2.1	Integration with Microsoft Defender/Sentinel (including support for parsing evidence) or ServiceNow Security Incident Response (including support for parsing observables) is required.
PIR2.2.2	The PIR tooling must support the purging of phishing messages (tenant-wide search and delete).
PIR2.2.3	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.

2.3 Reporting process

Nr.	Requirements regarding reporting process
PIR2.3.1	The native Microsoft functionality for sharing unwanted or suspicious messages must remain intact in parallel.
PIR2.3.2	The PIR tooling must provide feedback to reporters after assessment. For each report, a manual comment can be added by SOC to the user feedback.
PIR2.3.3	Any email communications by the PIR tooling (such as feedback on a report) must be sent on behalf of the Enexis.nl domain and must follow the Enexis corporate branding guidelines.
PIR2.3.4	The Contractor must allow modification of text within any user interfaces part of the reporting process.

3. Security reporting & performance insights

3.1 Security reporting & performance insights

Nr.	Requirements regarding Reporting Security reporting & Performance insights
3.1.1	The Contractor must provide real-time insights through a reporting dashboard, with download/export capability. Data that must at minimum be reported: • number of reports per team • type (simulation or real phishing) • threat categories and tactics • assessment (final classification)
3.1.2	Reporting must be possible for specific reporting periods, aggregated by at minimum: • organizational unit • department • function role • End user training performance • other groups, (manually) defined by Enexis
CP3.1.3	The CP tooling must provide the ability to show insight into the successful delivery of simulation messages, including whether it has been read.
3.1.4	End users must be able to consult personal information about their results for both simulations and real phishing.
CP3.1.5	The CP tooling ensures that training performance data is anonymized and not reasonably re-identifiable in any views or exports available to general user roles, with individually identifiable performance accessible only to users assigned a designated role.

4. Phishing simulation & Security training

4.1 Reporting Phishing simulation & Security training

Nr.	Requirements regarding reporting phishing simulation & security training
CP4.1.1	The CP tooling must train and measure all aspects of a user's response to a phishing simulation relevant for the attack vector. Including, but not limited to: • message replied to • attachment opened • hyperlink clicked • interaction on a landing page
CP4.1.2	Reports related to CP simulations should be handled within a dedicated simulation workflow, separate from the operational PIR process.

4.2 Campaign management

Nr.	Requirements regarding campaign management
CP4.2.1	The CP tooling must be capable of delivering phishing simulation campaigns automatically and at random, with and without manual intervention.
CP4.2.2	The CP tooling must include an up-to-date, actively maintained and continuously expanding library of varied phishing simulation templates that incorporates newly identified threat patterns and attack techniques.
CP4.2.3	All content must be provided both in Dutch and English. All video and audio material must be available in both languages. Only using subtitles isn't allowed.
CP4.2.4	The Contractor must provide functionality to convert real phishing messages sent to Enexis into training simulations.
CP4.2.5	Enexis must be able to propose a specific topic or content for a phishing simulation campaign.
CP4.2.6	The Contractor must provide the option for Enexis to initiate a simulation campaign, targeting specific groups.
CP4.2.7	The Contractor must offer an adaptive difficulty level tailored to End user training performance and potential learning path.
CP4.2.8	The Contractor must provide the option for Enexis to create its own simulated phishing messages.
CP4.2.9	The CP tooling must have a WYSIWYG editor and HTML editing capabilities for simulation messages and landing pages.
CP4.2.10	It must be possible to send simulations to specific target groups aggregated by at minimum: • organizational unit • department • function role • End user training performance • other groups, (manually) defined by Enexis
CP4.2.11	It must be possible to send simulations organization-wide in a single run, in batches.
CP4.2.12	It must be possible to send simulation messages entirely in Enexis corporate style.
CP4.2.13	It must be possible to fully or partially customize the landing page shown after clicking a link in a phishing message, based on Enexis' instructions.
CP4.2.14	When a login page is used during the phishing activity, it must reflect the corporate style of the requested login page.
CP4.2.15	Phishing simulations must be able to include images (such as QR codes).
CP4.2.16	The CP tooling must provide End users with clear, and actionable feedback following each simulation.