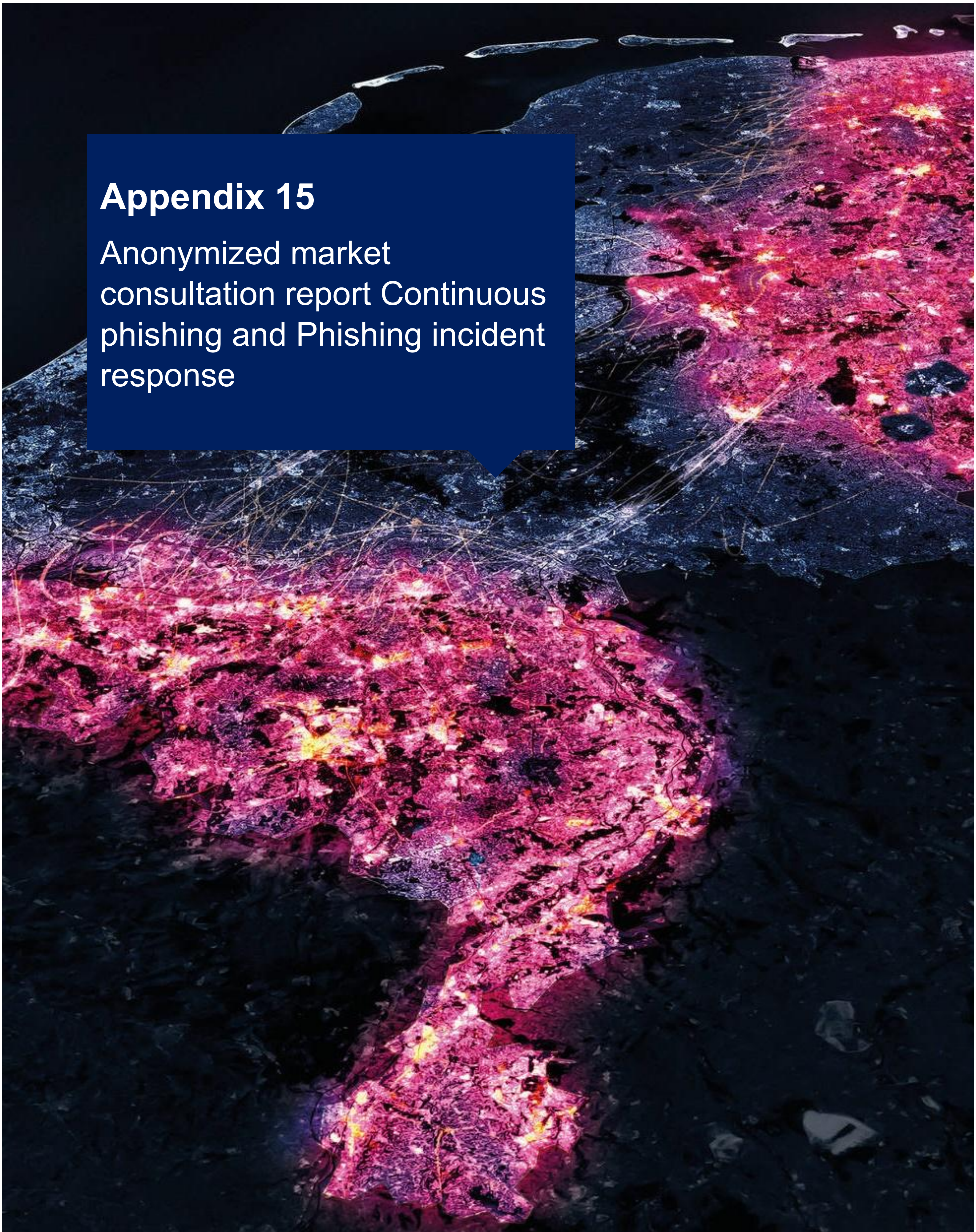
ENEXIS
PERSONEEL B.V.



Appendix 15

Anonymized market consultation report Continuous phishing and Phishing incident response

Introduction

Prior to the European tender procedure, Enexis conducted a market consultation in which eleven market parties participated. During this consultation, Enexis presented nineteen questions to the market and shared a draft structure of an initial version of the functional requirements. The outcome of the market consultation has been elaborated in this report. The results have been anonymized.

Draft schedule of requirements
Some of the feedback provided by the market participants on the draft schedule of requirements during the market consultation has been taken into account by Enexis in preparing the tender procedure. Several market parties indicated during the market consultation that Enexis could be more explicit in stating whether the requirement relates to Continuous phishing or Phishing incident response.

1. General questions

In this chapter, the market's responses to the general questions have been anonymized.

Question 1.1: Can you offer phishing incident response and phishing simulation, as mentioned in the introduction of the Market Consultation Document, as a single solution, or do you prefer two separate lots?
Ten of the eleven market parties indicated that they offer both phishing simulation and phishing incident response as a single integrated service.

Question 1.2: What trends do you currently observe in the market for continuous phishing and/or phishing incident response?
The market parties provide varying responses to this matter.

Question 1.3: Do you also offer an email security product (anti-phishing), and can this be part of your solution?
Several market parties indicate that they offer email security. A few market parties state that they do not provide this service.

Question 1.4: In what way do you, as a contractor, address employees onboarding and offboarding regarding user management?
The market parties provide varying responses to this matter.

Question 1.5: The contracting authority may wish to include a presentation/demo as part of the quality award criteria. What is your view on this, and what possibilities do you see in this regard?
All market parties respond positively to the idea of including a demo as part of the quality award criteria.

Question 1.6: From a GDPR point-of-view: How does your company handle customer (Enexis) generated data?
The market parties provide varying responses to this matter.

Question 1.7: In your experience, what is the required time (preparation, technology, and adoption) for successful implementation of your proposed solutions?
The market parties provide varying responses to this matter. The required time for successful implementation indicated by the market parties has a range from approximately two weeks to a maximum of twelve weeks.

Question 1.8: What is your view on the distinction between an end user's response to an awareness training (phishing simulation) email versus a real threat, and how should the end user understand how to respond/report appropriately in each of these situations?
The market parties provide varying responses to this matter.

Question 1.9: Enexis uses a multi-layered hierarchy of departments. Could you clarify whether the tool and its API limit the number of departments, and how many hierarchical layers can be supported for filtering?
Nearly all market parties indicate that there is no API limit to the number of departments.

2. Questions about phishing incident response

In this chapter, the market's responses to the questions about phishing incident response have been anonymized.

Question 2.1: With which incident management systems can your solution integrate and are there any other prerequisites?
Several market parties indicate that the solution they offer can integrate with platforms like ServiceNow, Jira, SOAR/SIEM, and additional platforms.

Question 2.2: (1) Which characteristics of emails are used for automatic analysis? (2) Do you have a particular vision about this? (3) Do you apply specific methodologies and techniques for this?
The market parties provide varying responses to this matter.

Question 2.3: What is your vision regarding automation, triage, and tuning in relation to the operational workload of SOC analysts?
The market parties provide varying responses to this matter.

3. Questions about phishing simulation

In this chapter, the market's responses to the questions about phishing simulation have been anonymized.

Question 3.1: (1) In what way and within what timeframe is an employee informed after making a mistake in the phishing simulation? (2) Is immediate feedback provided, for example via a pop-up, explanation page, or email? (3) Could you describe the process and provide examples of the feedback given to the end user? (4) Is this feedback customer editable for specific comments?
(1) Most market parties indicate that the employee is informed immediately after making a mistake during the phishing simulation. (2) Also, feedback is immediately provided by the market parties. (3) The market parties provide varying responses to this matter. (4) Some of the market parties offer the possibility to edit the phishing simulation based on given feedback.

Question 3.2: (1) How is the difficulty level of the simulations determined? (2) Are the simulations adaptive? (3) Do they adapt to the user's response/expertise level?
(1) Most of the market parties offer different difficulty levels in simulation training. (2) The market parties provide varying responses to this matter. Some market parties indicate that simulations are adaptive, while other market parties indicate that they do not offer this possibility. (3) Most market parties that offer adaptive simulations indicate that the simulations can be adaptive to the user's level of expertise.

Question 3.3: How do you ensure that the awareness training that you offer remains current and up to date?
The market parties provide varying responses to this matter.

Question 3.4: Do you also offer additional awareness trainings or e-learnings based on the results? If so, how do you deliver these?
All the market parties offer (e)-learnings based on the results.

Question 3.5: How do you take care of training fatigue and engagement?
The market parties provide varying responses to this matter.

Question 3.6: How does the contractor measure the learning effect?
The market parties provide varying responses to this matter.

4. Question about the licensing model

In this chapter, the market's responses to the question about the licensing model have been anonymized.

Question 4.1: What does the structure of your licensing model look like?
Most of the market parties offer a licensing model based on the number of active users per year. Some market parties offer additional supplementary licensing models.