



Tender

T182560 Market Consultation Continuous phishing and Phishing Incident response

#	Referentie	Publicatiedatum
1	2. What do we ask? The participating market...	08 jan 2026 (do), 17:22
Vraag Is Enexis using ServiceNow as an incident management system?		
Antwoord Yes, Enexis is using the Incident Management application for the ITIL Incident Management process and the Security Incident Response application for operational Security Incident Management.		
2	2. What do we ask? The participating market...	08 jan 2026 (do), 17:22
Vraag How many unique users does Enexis have?		
Antwoord Approximately 8000 users.		
3	2. What do we ask? The participating market...	08 jan 2026 (do), 17:22
Vraag Can the solution be delivered as a service or does it have to be a tool?		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		
4	2. Why a Market ConsultationBefore publishi...	08 jan 2026 (do), 17:22
Vraag Can you clarify whether Enexis has a preference for a single integrated solution covering both phishing simulations and phishing incident response, or whether two separate tools or lots are considered equally acceptable in the future tender?		
Antwoord Enexis wants to gather insights from the market consultation on what the market can offer in this regard. Based on the market response Enexis will make a decision.		
5	2. Why a Market ConsultationBefore publishi...	08 jan 2026 (do), 17:22
Vraag The draft requirements mention integration with Microsoft Defender/Sentinel or ServiceNow Security Incident Response. Can you indicate which platform is currently leading within the Enexis environment, and whether support for both platforms simultaneously is required or optional?		
Antwoord ServiceNow and Sentinel are currently working indepedent from eachother. While ServiceNow is currently leading for administering alerts or reports escalated for further analysis/response, triage and automation on reported phishing emails could take place in Sentinel/Defender, before being escalated to a security incident in ServiceNow if required.		

# 6	Referentie 2. Why a Market ConsultationBefore publisi...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag With regard to the parsing of evidence and observables, can you clarify which specific data elements are considered mandatory (for example email headers, URLs, attachments, user context, campaign identifiers), and whether a standardized data format or schema is expected?		
Antwoord The data format or schema will be dependant of the target system (Sentinel or ServiceNow), taking into account any compatibility requirements and reliability. Based on our functional requirement, we would like to be advised about possible technical approaches for integrating your tool. For mapping evidence (Defender/Sentinel) / observables (ServiceNow Threat Intelligence) we expect at least internet message ID, email addresses (sender, recipients and CC headers, strings in message body), URLs and attachments (file name, hash).		
# 7	Referentie 2. Why a Market ConsultationBefore publisi...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag The requirements refer to the ability to purge malicious emails. Can you clarify whether this includes tenant-wide search and delete, including shared and functional mailboxes, and whether remediation actions must be executed directly via Microsoft APIs or may be orchestrated through an integrated workflow?		
Antwoord It concerns tenant-wide search and delete for all mailboxes Defender/Exchange Online has the capability for. Please note that we are currently in the market consultation phase, in which we are exploring the available functional capabilities on which we can base our final requirements. Enexis is therefore not yet able to provide an answer to your question about technical requirements.		
# 8	Referentie 2. Why a Market ConsultationBefore publisi...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag Regarding phishing reporting, does Enexis expect a single unified reporting button for both simulated and real phishing emails, or is a functional separation in user experience acceptable provided that simulated emails are excluded from the regular incident workflow?		
Antwoord Our preliminary functional requirement is that the awareness training must not negatively affect employees' clarity about reporting real potential threats. If sending actual emails is part of your training product, we therefore expect a single reporting button for both to be necessary, since recipients will not be able to distinguish whether it concerns training or a real threat. However, we are open to any alternative solutions that still meet our functional requirement.		
# 9	Referentie 2. Why a Market ConsultationBefore publisi...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag Can you clarify the expected form of feedback to end users after reporting a phishing email (for example immediate in-client feedback versus follow-up email), and to what extent Enexis requires full control over content, tone of voice and branding of this communication?		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		
# 10	Referentie 2. Why a Market ConsultationBefore publisi...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag For shared and functional mailboxes, should these mailboxes only be able to report phishing emails, or should they also be fully included in statistics, dashboards and incident response workflows?		
Antwoord We require reporting suspicious emails received in shared and functional mailboxes to be similar to employees as with emails received in their personal mailbox. The subsequent workflow and insights ideally should not differ based on the type of mailbox. Non-personal mailboxes will not need to be targeted for training though, which makes inclusion in the related statistics unnecessary.		

# 11	Referentie 2. Why a Market ConsultationBefore publishi...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag With respect to identity and provisioning, which system is considered the authoritative source (for example Entra ID or an HR system), and is SCIM-based lifecycle management a hard requirement or a preferred option alongside SSO?		
Antwoord OMADA Cloud is used for IAM. Provisioning by it is usually performed through groups in Microsoft Entra ID, both having integration capabilities.		
# 12	Referentie 2. Why a Market ConsultationBefore publishi...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag The reporting requirements mention insight into whether an email was “read”. Can you clarify how Enexis defines this metric, and whether alternative indicators such as delivery, open or user interaction are acceptable where technical or privacy constraints apply?		
Antwoord With question 3.1.2 regarding training metrics, we wish to know about nonrespondents, whether they have actually seen the simulation email. This to get more accurate insight into the ratio of employees not engaged in training, versus employees simply not monitoring their mailbox well enough to notice them.		
# 13	Referentie 2. Why a Market ConsultationBefore publishi...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag Which stakeholder groups within Enexis are expected to actively use dashboards (for example SOC, awareness team, management), and is role-based separation of dashboards required?		
Antwoord Both for participant-like stakeholder-focused insights and for security team stakeholders separation will likely be required, depending on the information they provide.		
# 14	Referentie 2. Why a Market ConsultationBefore publishi...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag The survey refers to “fully managed” phishing simulations. Can you clarify whether this includes only campaign execution and content management, or also continuous tuning, escalation logic and periodic reporting?		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		
# 15	Referentie 2. Why a Market ConsultationBefore publishi...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag How does Enexis envision the division of responsibilities between the supplier and Enexis for phishing simulations, phishing incident response and ongoing optimisation of detection and response processes?		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		

# 16	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag What is the estimated value of the procurement based on the current situation?		
Antwoord This is determined based on market research and historical data. Enexis is also doing market research on the pricing for this solution.		
# 17	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag How will the budget range for the future tender be determined? Is Enexis conducting market research on pricing for this solution as well?		
Antwoord This is determined based on market research and historical data. Enexis is also doing market research on the pricing for this solution.		
# 18	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag What are the main functions Enexis is missing in the current solution that is being used?		
Antwoord Some of the functionality we desire and may currently lack have been included in our questions and preliminary requirements. Through this market consultation, we hope to identify any additional functionalities we may wish to pursue.		
# 19	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 1. Welke functionaliteiten of capabilities van de huidige oplossing sluiten volgens Opdrachtgever onvoldoende aan op de gewenste toekomstige situatie?		
Antwoord Some of the functionality we desire and may currently lack have been included in our questions and preliminary requirements. Through this market consultation, we hope to identify any additional functionalities we may wish to pursue.		
# 20	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 2. Welke verbeteringen beoogt Opdrachtgever met deze aanbesteding te realiseren?		
Antwoord Some of the functionality we desire and may currently lack have been included in our questions and preliminary requirements. Through this market consultation, we hope to identify any additional functionalities we may wish to pursue.		
# 21	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 3. Welke uitbreidingen beoogt Opdrachtgever met deze aanbesteding te realiseren?		
Antwoord Some of the functionality we desire and may currently lack have been included in our questions and preliminary requirements. Through this market consultation, we hope to identify any additional functionalities we may wish to pursue.		

# 22	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 4. Mag Opdrachtnemer ervan uitgaan dat Opdrachtgever zijn bestaande oplossing wenst te vervangen? Zo nee, licht toe.		
Antwoord Enexis currently holds a contract for both solutions until December 31, 2026. Following this period, Enexis intends to enter into a new agreement. As Enexis is subject to the European public procurement regulations, a tendering procedure will be conducted after the market consultation.		
# 23	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 5. Welke specifieke onderdelen van de huidige oplossing wenst Opdrachtgever te vervangen?		
Antwoord Some of the functionality we desire and may currently lack have been included in our questions and preliminary requirements. Through this market consultation, we hope to identify any additional functionalities we may wish to pursue.		
# 24	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 6. Op welke wijze is de transitie naar een nieuwe oplossing voorzien?		
Antwoord We are currently still in the market consultation phase. This will strongly depend on the chosen solution.		
# 25	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 7. In hoeverre is voor de transitie naar de nieuwe oplossing een uitgewerkt transitie- en exitplan beschikbaar dat onderdeel wordt van de aanbestedingsdocumentatie?		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		
# 26	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 8. Hoe zijn phishingcampagnes momenteel ingericht binnen Opdrachtgever (aub ingaan op de volgende 3 elementen: frequentie, doelgroepen, differentiatie)?		
Antwoord The current method is irrelevant. With this market consultation we hope to learn what the options are.		

# 27	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 9. Welke verbeteringen of doorontwikkelingen acht Opdrachtgever wenselijk met betrekking tot phishingcampagnes?		
Antwoord Some of the functionality we desire and may currently lack have been included in our questions and preliminary requirements. Through this market consultation, we hope to identify any additional functionalities we may wish to pursue.		
# 28	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 10. Wat verstaat Opdrachtgever exact onder on- en offboarding? Wil Opdrachtgever aub de use-case(s) beschrijven?		
Antwoord By that we refer to account lifecycle management / provisioning.		
# 29	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 11. Mag Opdrachtnemer ervan uitgaan dat de on- en offboarding van nieuwe gebruikers automatisch dient te verlopen? Zo nee, licht toe.		
Antwoord Please mind we are currently still in the market consultation phase. As described, we do desire this to happen automated in any way.		
# 30	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 12. Mag Opdrachtnemer ervan uitgaan dat het toepassen van bestaande campagnes of trainingen op nieuwe medewerkers geautomatiseerd dient te gebeuren? Zo nee, licht toe.		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		
# 31	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 13. Hoe is de huidige SOC-organisatie van Opdrachtgever ingericht (intern, hybride of uitbesteed)?		
Antwoord To Enexis, this question seems irrelevant for the purpose of the market consultation.		
# 32	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 14. Welke overwegingen liggen ten grondslag aan de keuze voor het huidige SOC?		
Antwoord To Enexis, this question seems irrelevant for the purpose of the market consultation.		

# 33	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 15. Wat is de huidige SOC-oplossing (bijvoorbeeld Sentinel, Splunk of QRadar etc..)?		
Antwoord Enexis uses more than one application/platform tied to cyber security operations in general. Relevant to phishing incident response will be Microsoft Sentinel/Defender (SIEM) and ServiceNow Security Operations (security incident management).		
# 34	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 16. Welke functionele en procesmatige eisen stelt Opdrachtgever aan de integratie met ServiceNow, bijvoorbeeld ten aanzien van incidentafhandeling, workflowautomatisering en rapportages?		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		
# 35	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 17. Vraag 2.3 verwijst naar SOC-analistbetrokkenheid. Welke specifieke use case wenst Opdrachtgever hiermee te adresseren?		
Antwoord Question 2.3 stems from the common situation in which a large number of phishing reports are submitted, but the majority do not indicate any danger or don't require action. We are interested to know about your vision (on which your product is likely based) regarding the balance between capturing absolutely every true positive and the sustainable, highly efficient use of human capacity for managing actual threats. In other words: where, in your view, should an organisation position itself on the spectrum between A) maximum certainty by checking every single report, and Z) full automation?		
# 36	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 18. Gezien de wens en/of noodzaak tot integratie heeft Opdrachtnemer behoefte aan een architectuuroverzicht (beschrijving van IAM-oplossing, Endpoint Detection & Response (EDR)-oplossing, externe e-mailsecurity oplossing, interne e-mailsecurity oplossing, Network Detection & Respons (NDR)-oplossing, firewall(s), Office 365 collaboration security en Office 365 mail security). Is Opdrachtgever bereid deze beschikbaar te stellen? Zo nee, licht toe.		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		
# 37	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 19. Welke documentatie over de huidige inrichting (zoals processen, use cases, integraties en configuraties) stelt Opdrachtgever beschikbaar aan inschrijvers, en op welk detailniveau?		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		

# 38	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 20. Wat verstaat Opdrachtgever exact onder het begrip multilayer (vraag 1.9)?		
Antwoord With this, Enexis wishes to indicate that the organizational structure has been segmented.		
# 39	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 21. Welke use case wenst Opdrachtgever te adresseren met betrekking tot multilayer?		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		
# 40	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 22. Mag Opdrachtnemer ervan uitgaan dat nudges vereist zijn binnen de oplossing? Zo nee, licht toe.		
Antwoord We expect the contractor to be a specialist in positive influence, which is why, as the client, we will not insist on the use of any specific technique.		
# 41	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag Een nudge is een beknopt bericht gericht aan individuele medewerkers dat op het juiste moment wordt verzonden, bijvoorbeeld wanneer iemand een klikbare phishinglink opent, een simulatietest succesvol afrondt of zich aan training houdt. Het doel is gedrag bij te sturen of positief te bekrachtigen. Nudges zijn gebaseerd op de gedragswetenschappelijke nudge theory.		
Antwoord Thank you for your explanation, it is appreciated.		
# 42	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 23. Aangezien de markt verschuift naar de noodzaak van realtime risicobeoordeling van gebruikers en daarop dynamisch anticiperen, beschouwt Opdrachtnemer dit als een essentieel onderdeel van de geboden oplossing. Mag Opdrachtnemer ervan uitgaan dat dit een eis is? Zo nee, licht toe.		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		

# 43	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 24. De markt ontwikkelt zich richting oplossingen die een single pane of glass bieden voor gebruikers- en gedragsdata uit verschillende oplossingen, zoals e-mailsecurity, phishingoplossingen en andere securitytools (bijvoorbeeld EDR). Mag Opdrachtnemer ervan uitgaan dat dit een eis is? Zo nee, licht toe.		
Antwoord This is stated in requirement 2.2.1 Appendix A.		
# 44	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 25. Welke rol ziet Opdrachtgever voor role-based access control (RBAC) binnen awareness- en phishingcampagnes?		
Antwoord In light of the number of questions received and the current market exploration phase Enexis is in, we do not consider responding to this question relevant at this stage.		
# 45	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 26. Welke rol ziet Opdrachtgever voor doelgroepsegmentatie binnen awareness- en phishingcampagnes?		
Antwoord This is a question that the contractor will have to answer for themselves and include in their proposition.		
# 46	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 27. In welke mate is de huidige dienstverlening gebaseerd op maatwerkprocessen, maatwerkconfiguraties of propriëtaire tooling?		
Antwoord We deem the current implementation irrelevant to our market consultation. With this market consultation we hope to learn what the options are.		
# 47	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 28. Welke impact heeft dit maatwerk volgens Opdrachtgever op de overdraagbaarheid naar een nieuwe leverancier?		
Antwoord We expect the current implementation to pose little complexity.		
# 48	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 29. Mag Opdrachtnemer ervan uitgaan dat Opdrachtgever vereist dat nieuwsbrieven of phishing simulaties automatisch gemarkeerd kunnen worden om het SOC te ontlasten? Zo nee, licht toe.		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		

# 49	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 30. Mag Opdrachtnemer ervan uitgaan dat de gewenste oplossing, gezien de noodzaak om phishingrisico's integraal te mitigeren, ook bescherming biedt voor interne e-mailstromen? Zo nee, licht toe.		
Antwoord At the moment this is not within the scope defenition, though we are certainly interested in such capability.		
# 50	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 31. Mag Opdrachtnemer ervan uitgaan dat de gewenste oplossing, gezien de noodzaak om phishingrisico's integraal te mitigeren, ook bescherming biedt voor externe e-mailstromen? Zo nee, licht toe.		
Antwoord At the moment this is not within the scope defenition, though we are certainly interested in such capability.		
# 51	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 32. Mag Opdrachtnemer ervan uitgaan dat de oplossing phishingcampagnes kan aanbieden in minimaal 20 talen, waaronder Nederlands, Frans en Duits, zodat medewerkers in hun moedertaal kunnen worden getraind? Zo nee, licht toe.		
Antwoord No. We consider it only necessary to train people on the few languages that are typical for our organization and contacts to use. See also requirement 1.2 in Apendix A.		
# 52	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 33. Mag Opdrachtnemer ervan uitgaan dat de oplossing vooraf gedefinieerde templates biedt voor verschillende aanvalsthema's (bijvoorbeeld Business E-mail Compromise (BEC), social media en betalingsfraude), en dat deze templates eenvoudig aanpasbaar zijn? Zo nee, licht toe.		
Antwoord This is a question that the contractor will have to answer for themselves and include in their proposition.		
# 53	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 34. Mag Opdrachtnemer ervan uitgaan dat de oplossing phishingcampagnes kan segmenteren op basis van risicoprofiel, functie en locatie, inclusief ondersteuning voor meertalige distributie binnen één campagne? Zo nee, licht toe.		
Antwoord This is a question that the contractor will have to answer for themselves and include in their proposition.		

# 54	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 35. Mag Opdrachtnemer ervan uitgaan dat de oplossing dynamische waarschuwingen en contextuele feedback biedt tijdens een klikactie (real-time user coaching), naast traditionele landing pages? Zo nee, licht toe.		
Antwoord This is a question that the contractor will have to answer for themselves and include in their proposition.		
# 55	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 36. Mag Opdrachtnemer ervan uitgaan dat de oplossing naast e-mail ook andere communicatiekanalen (bijvoorbeeld Teams of Slack) kan simuleren binnen phishingcampagnes, om een realistisch dreigingsbeeld te creëren? Zo nee, licht toe.		
Antwoord This is a question that the contractor will have to answer for themselves and include in their proposition.		
# 56	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 37. Mag Opdrachtnemer ervan uitgaan dat de oplossing verschillende moeilijkheidsgraden in phishingcampagnes ondersteunt, zodat gebruikers geleidelijk worden uitgedaagd? Zo nee, licht toe.		
Antwoord This is a question that the contractor will have to answer for themselves and include in their proposition.		
# 57	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 38. Mag Opdrachtnemer ervan uitgaan dat verdachte content (phishing, malware, BEC) automatisch kan worden gedetecteerd en verwijderd uit alle relevante communicatiekanalen, inclusief interne e-mailstromen? Zo nee, licht toe.		
Antwoord Please review preliminary requirement 2.2.2, outlining the need for such capability in regards to emails. Though we are certainly interested in additional capabilities.		
# 58	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 39. Mag Opdrachtnemer ervan uitgaan dat de oplossing geavanceerde dreigingsanalyse toepast (zoals sandboxing, AI en URL-scanning) op zowel inkomende als interne e-mailcommunicatie? Zo nee, licht toe.		
Antwoord Please refer to our answer in question 50 in regards to email protection. In respect to our preliminary requirement 2.1.2 regarding automatic initial assesment of reported mails, the mentioned techniques could be applicable.		

# 59	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 40. Mag Opdrachtnemer ervan uitgaan dat de oplossing geïntegreerde incident response biedt, inclusief automatische triage en koppeling met SIEM/XDR, voor zowel externe als interne e-mailincidenten? Zo nee, licht toe hoe.		
Antwoord Please refer to our preliminary requirements in section 2 of Appendix A.		
# 60	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 41. Mag Opdrachtnemer ervan uitgaan dat de oplossing phishing awareness combineert met geautomatiseerde incident response en interne e-mailsecurity binnen één geïntegreerd platform? Zo nee, licht toe.		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		
# 61	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 42. Mag Opdrachtnemer ervan uitgaan dat de oplossing realtime dreigingsinformatie kan delen met het SOC en bestaande securitytools? Zo nee, licht toe.		
Antwoord This is currently not one of our requirements, but feel free to include this in your proposition if according to you this could be very beneficial to us.		
# 62	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 43. Mag Opdrachtnemer ervan uitgaan dat de gewenste oplossing gebruikmaakt van Europese datacenters en volledige AVG/GDPR-compliance garandeert voor alle functionaliteiten (training, e-mailsecurity en interne e-mailsecurity)? Zo nee, licht toe.		
Antwoord Enexis will incorporate the relevant non-functional requirements into the tender documentation. At this stage of the market consultation, Enexis is not in a position to provide a definitive response regarding these requirements.		
# 63	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 44. Mag Opdrachtnemer ervan uitgaan dat alle data van de gewenste oplossing, inclusief gebruikersstatistieken en incidentinformatie, binnen de EU wordt opgeslagen en verwerkt? Zo nee, licht toe.		
Antwoord Enexis will incorporate the relevant non-functional requirements into the tender documentation. At this stage of the market consultation, Enexis is not in a position to provide a definitive response regarding these requirements.		

# 64	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 45. Mag Opdrachtnemer ervan uitgaan dat de gewenste oplossing uitgebreide rapportages biedt over klikgedrag, risicoscores en campagne-effectiviteit, inclusief exportmogelijkheden naar SIEM/XDR? Zo nee, licht toe.		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		
# 65	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 46. Mag Opdrachtnemer ervan uitgaan dat de gewenste oplossing dashboards biedt waarmee securityteams realtime inzicht krijgen in dreigingen en gebruikersgedrag? Zo nee, licht toe.		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		
# 66	Referentie 1. Welcome to the Market Consultation Conti...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag 47. Gezien het aantal vragen en de verwachting dat er vervolgvragen zullen volgen op de eerste Nota van Inlichtingen, ziet Opdrachtnemer aanleiding om de planning te heroverwegen. Mag Opdrachtnemer ervan uitgaan dat de deadline voor het indienen van de antwoorden op de marktconsultatie wordt verschoven? Zo nee, licht toe.		
Antwoord Enexis will not amend the schedule as a result of this clarification note. This stage pertains to a market consultation intended to collect feedback on the draft set of requirements and to address submitted questions. It does not constitute the commencement of the tendering procedure.		
# 67	Referentie 2. What do we ask? The participating market...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag Regarding requirement 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"), we would like to seek clarification on the intent of this requirement. The detection of real-world phishing emails received by multiple users and the broadcasting of alerts based on such events typically falls within the functional scope of a Phishing Incident Response solution. As the DRAFT Schedule of Requirements distinguishes between Phishing Simulation and Phishing Incident Response, could Enexis please clarify whether this requirement is intended to be addressed within the Incident Response scope (or lot), rather than the Phishing Simulation capability?		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		
# 68	Referentie 2. What do we ask? The participating market...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag In Chapter 4, titled "Phishing simulation & Security training", could you please clarify how Enexis defines the relationship between phishing simulation and security training? More specifically, does Enexis consider phishing simulation itself as a form of security training, or is Enexis also explicitly looking for a broader or integrated security awareness training solution in addition to the simulation capability? This clarification would help us better understand whether the requirements in this chapter primarily relate to the simulation offering, a security training solution, or a combination of both.		
Antwoord We are currently still in the market consultation phase. Enexis is therefore not yet able to provide an answer to your question.		

# 69	Referentie 2. What do we ask? The participating market...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag Regarding Question 1.8, could Enexis please clarify the underlying objective of distinguishing between an end user's response to a phishing simulation email and a real phishing email? Specifically, is Enexis aiming for a particular behavioural, operational or reporting outcome with this distinction? This clarification will help us align our response with the intended use and evaluation criteria.		
Antwoord We know that some tools on the market sending simulation mails have their own, separate workflow for interacting with them. Otherwise potentially reporting simulated threats to the security team through the default submission flow could require employees to distinguish between training emails and potential real threats, as well as to understand the different ways in which they are expected to respond in each case. We would to know if, for example, you deem a single report message button for both types to be necessary or what alternatives you propose that work just as well.		
# 70	Referentie 2. Why a Market ConsultationBefore publishi...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag In the market consultation document it is stated that Enexis currently works with Hoxhunt until the end of December 2026. Could you clarify which specific services are currently delivered under this engagement (e.g. phishing simulation, phishing incident response, or both)?		
Antwoord Enexis currently holds a contract for both solutions until December 31, 2026. Following this period, Enexis intends to enter into a new agreement. As Enexis is subject to the European public procurement regulations, a tendering procedure will be conducted after the market consultation.		
# 71	Referentie 2. Why a Market ConsultationBefore publishi...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag Additionally, could you indicate Enexis has a preference for continuing with a single integrated solution, or is considering separating phishing simulation and phishing incident response into distinct lots in a future procurement? This information would help us assess the relevance and suitability of our participation in a potential follow-up tender.		
Antwoord Following this market consultation, Enexis intends to decide whether to procure the solution as a single integrated lot or as two separate lots. Enexis currently does not have insight into what the market can offer in this regard.		
# 72	Referentie 2. What do we ask? The participating market...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag In the text of Appendix A is stated: 'Emails/campaigns already assessed by Enexis (benign or malicious) must be handled automatically'. Could you clarify what is meant by "automatically" in this context? How are these emails or campaigns currently assessed, and which system(s) are used for this assessment?		
Antwoord With that we mean that new reports regarding a campaign already assessed and completed by our security team, don't have to be manually resolved again with each instance, but instead are automatically resolved following the same verdict. This will mostly apply to safe emails not getting deleted and blocked and therefore later on can still get reported by other recipients.		
# 73	Referentie 2. Why a Market ConsultationBefore publishi...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag Market consultation document: 'With the current implementation, SOC analysts are reviewing any automatically escalated reports in Hoxhunt's web application and documenting their findings and actions in there.' Is Enexis looking for a solution that can also document these findings? Additionally, does the SOC use any other systems to review or handle flagged items?		
Antwoord Please refer to preliminary requirement 2.2.1. We desire to administer phishing incidents in the existing alert or incident workflows and panes (respectively Microsoft security portal or ServiceNow Security Incident Response).		

# 74	Referentie 1. Instruction This instruction intents to ...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag Will responses to the questions be made public, or will they be shared exclusively with the parties that submitted them?		
Antwoord This clarification note will be anonymized and published on Mercell. The Appendix C – Survey completed by market participants will not be published. The overall outcome of the market consultation will be shared in an anonymized summary report as an annex to the tender documentation.		
# 75	Referentie 2. What do we ask? The participating market...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag What incident management system is used by Enexis? And what is the definition of an incident management system for Enexis?		
Antwoord Enexis on the ServiceNow platform is using the Incident Management application for the ITIL Incident Management process and the Security Incident Response application for operational Security Incident Management.		
# 76	Referentie 2. What do we ask? The participating market...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag Is Enexis using Microsoft Defender? If yes: what is the added value of an email (malware) detection/protection system?		
Antwoord To Enexis, this question seems irrelevant for the purpose of the market consultation.		
# 77	Referentie 2. What do we ask? The participating market...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag Current & Desired solution: What are the most important reasons to replace the Hoxhunt solution? What are the pain points with the current solution that Enexis explicitly wants to resolve?		
Antwoord Enexis currently holds a contract for both solutions until December 31, 2026. Following this period, Enexis intends to enter into a new agreement. As Enexis is subject to the European public procurement regulations, a tendering procedure will be conducted after the market consultation. We choose not to elaborate on aspects in which the current product may be lacking. Some of the functionality we desire and may currently lack have been included in our questions and preliminary requirements.		
# 78	Referentie 2. What do we ask? The participating market...	Publicatiedatum 08 jan 2026 (do), 17:22
Vraag SOC workload & volumes - What is the average and peak volume of reported emails per month today? - What percentage is currently false positives vs real threats?		
Antwoord To Enexis, these questions seem irrelevant for the purpose of the market consultation.		

#	Referentie	Publicatiedatum
79	2. What do we ask? The participating market...	08 jan 2026 (do), 17:22
Vraag SLA & response times: - Are there internal SLAs or regulatory response targets for phishing incident handling that the solution should support or report on?		
Antwoord As described, we desire phishing incidents to integrate with our existing systems for either SIEM or Security incident management (preliminary requirement 2.2.1). These will already be capable of tracking and reporting on incident handling performance metrics. In any other way, we would indeed still be capable of reporting on operational performance. Not having any significant delay in the forwarding of phishing incidents (technical) will also be important in this regard.		