Marketconsultation Threat Intelligence Platform, Memorandum of Information

4-nov-26

#	Question	Answer
1	Hoeveel servers, eindpunten, netwerkapparaten, cloudresources, virtuele machines, OT-assets en andere ondersteunde assetsoorten worden er binnen het beveiligingslandschap van Enexis gebruikt?	Enexis' IT and OT landscape consists of a combination of cloud environments, including Azure and AWS, and on-premises technologies. In total, the landscape comprises many thousands of endpoints and assets of various types.
2	Deadline: The notice gives 04/11/2026 23:59 as the deadline for answers. Section 4.1 gives 11/11/2026 for the written response and 04/11 for the Memorandum of Information. Please confirm which deadline applies.	The deadline for submission of the written response to the consultation paper is 11 November 2026, as stated in Section 4.1. The date of 4 November 2026 concerns the publication of the Memorandum of Information.
3	Submission channel: Section 4.2 says responses go via Mercell, but the notice gives TenderNed as the submission address. Please confirm the channel and provide the Mercell link and registration details, if Mercell applies.	TenderNed is the correct and applicable submission channel. The reference to Mercell in Section 4.2 is incorrect. Tenderers must submit their responses via TenderNed.
4	Follow-up sessions (weeks 47–48): How will participants be selected, and will sessions be on-site or remote?	Enexis may invite market participants based on the content and relevance of the responses received and the topics on which further exploration is desired.Follow-up sessions may be conducted either on-site or remotely; Enexis will decide later on.
5	IT and OT SOC (2.1): Will one platform serve both SOCs? Are there connectivity limits for the OT SOC, such as isolated or offline networks, that affect the deployment model (Q1)?	Enexis has a shared CTI team supporting both the IT and OT SOCs. The TIP will primarily be used by the CTI team and will therefore indirectly support both SOCs. Enexis currently envisages a cloud/SaaS deployment, with potential connections to the IT and OT environments. OT connectivity may be subject to specific limitations depending on the deployment and integration scenario.
6	Current tooling (Q7, Q8, Q9): Which SIEM, SOAR, EDR and ticketing tools are in use?	Enexis currently uses Sentinel, Elastic and Defender for SIEM and EDR purposes. ServiceNow is the primary ticketing system in use.
7	Intelligence providers (Q3): Which commercial, government and sector sources do you use now or plan to use?	Enexis currently uses a mix of threat intelligence sources, which we continuously aim to improve.
8	Hosting (Q2): What distinction do you draw between “SaaS” and “Cloud”? Are there requirements for EU data residency, certifications, or limits on using AI to process Enexis data?	Enexis considers a cloud deployment to be a deployment within the Enexis cloud environment (Azure or AWS), whereas a SaaS deployment is hosted and managed by the selected provider. Enexis currently prefers a SaaS deployment, although no definitive choice has been made. EU data residency is considered an option. Specific requirements regarding certifications and the use of AI have not yet been defined.
9	Which outcomes or improvements would Enexis use to determine that implementation of the Threat Intelligence Platform has been successful?	Enexis considers the implementation successful when the CTI team can use the TIP as a single pane of glass from which most CTI activities can be performed, reducing the need to work across multiple tools and interfaces.
10	Where are the most significant manual steps, tool switches or process bottlenecks in the current intelligence lifecycle?	The current intelligence lifecycle is still developing. Standardised templates for CTI products are not yet in place, and the quality of data feeds requires improvement. We want to use a TIP as a centralized workplace, supporting a high level of automation where possible.
11	Besides the four CTI-focused SOC analysts, which user groups are expected to interact directly with or consume information from the TIP?	In addition to the CTI team, Security Engineering may occasionally interact directly with the TIP. Other CTI stakeholders are expected to primarily consume CTI products delivered by the CTI team rather than interact directly with the platform.
12	Should the TIP provide a common workspace across the IT and OT SOC environments, or are there requirements for logical or technical separation?	Yes. The TIP is expected to provide a common workspace for the Enexis CTI team across both the IT and OT SOC environments.
13	Which external Threat Intelligence providers, feeds and subscriptions are currently used and should be considered for integration?	See the answer to question 7
14	Which existing SIEM, SOAR and other relevant SOC or security platforms should suppliers consider when describing integration capabilities?	See the answer to question 6
15	How is MISP currently used within the CTI/SOC environment, and what role should it have alongside the future TIP?	MISP is currently used to provide IOC's to both SOC's
16	Are there Enexis-specific classification, data-handling, data-residency or segregation requirements that the TIP must support beyond TLP?	No. Enexis currently has no additional specific requirements beyond TLP in this regard.
17	Does Enexis expect existing intelligence, reports, indicators, actor information or other CTI content to be migrated into the new TIP? If so, what indicative volumes and formats should be considered?	At this stage, Enexis does not anticipate migrating existing CTI content to the new TIP. In general, we aim to utilize common CTI formats.
18	Are there particular use cases or integrations Enexis would like suppliers to demonstrate or substantiate when describing their solution?	Enexis would like suppliers to demonstrate how MISP can be integrated with the TIP, both as a source of input and as an output channel, and how a TIP solution supports the CTI analist in tracking threat actor activty and reporting on said activity.
19	Deadline: The notice gives 04/11/2026 23:59 as the deadline for answers. Section 4.1 gives 11/11/2026 for the written response and 04/11 for the Memorandum of Information. Please confirm which deadline applies.	See the answer to question 2
20	Submission channel: Section 4.2 says responses go via Mercell, but the notice gives TenderNed as the submission address. Please confirm the channel and provide the Mercell link and registration details, if Mercell applies.	See the answer to question 3
21	Follow-up sessions (weeks 47–48): How will participants be selected, and will sessions be on-site or remote?	See the answer to question 4
22	IT and OT SOC (2.1): Will one platform serve both SOCs? Are there connectivity limits for the OT SOC, such as isolated or offline networks, that affect the deployment model (Q1)?	See the answer to question 5
23	Current tooling (Q7, Q8, Q9): Which SIEM, SOAR, EDR and ticketing tools are in use?	See the answer to question 6
24	Intelligence providers (Q3): Which commercial, government and sector sources do you use now or plan to use?	See the answer to question 7
25	Hosting (Q2): What distinction do you draw between “SaaS” and “Cloud”? Are there requirements for EU data residency, certifications, or limits on using AI to process Enexis data?	See the answer to question 8
26	Ingestion of Feeds: What kind of Feeds are you looking to integrate?	See the answer to question 7
27	Ingestion of Feeds: How many commercial feeds are you considering integrating?	Enexis aims to leverage a mix of different feeds. Over time, the number of feeds (both open and closed source) may change.
28	Ingestion of Feeds: How many OSINT feeds are you considering integrating? How many Government feeds are you considering integrating?	See the answer to question 27
29	Ingestion of Feeds: What is the expected volume of IoCs expected?	Enexis has no indicative volume of IoCs defined at this stage.
30	Ingestion of Feeds: Will you bring your own API key for the commercial feeds or are you looking to do a buy through via the TIP supplier?	Enexis will provide its own API keys.
31	Enrichment: Is Enrichment functionality required? If yes, what kind of supplier do you expect an OOTB integration with?	Enexis has not yet defined specific requirements regarding enrichment functionality or OOTB integrations. We welcome market input and recommendations on this subject.
32	Downstream integration: Besides SIEM/SOAR, what other security systems would be required to be integrated?	Integration with SIEM/SOAR and EDR is required. Firewall integration may be an optional use case in the future.
33	Downstream integration: Is it expected to integrate to Vulnerability Management system?	No specific requirements have been defined at this stage. Enexis welcomes market input on potential integrations with Vulnerability Management systems.
34	Downstream integration: Assume that the Solution analyzes the log telemetry in the customer environment and notices that there are malicious IOCs that are in the configured feeds, would you like to be notified about it? Would you like the IoCs to be automatically disseminated to the other security controls.	Enexis envisages a solution in which the TIP aggregates multiple CTI sources and provides, among other capabilities, a consolidated IoC feed to the Enexis security stack across both the IT and OT environments. IoC matching, alerting and notification will remain within the IT and OT SIEMs. Enexis log data must remain within the Enexis environments and will therefore not be uploaded to a SaaS-based TIP. Although deployment models that allow Enexis data to be processed within the Enexis IT cloud or OT on-premises environment may be technically possible, such a deployment model is currently not preferred.
35	Threat Actor Cards: Will the analyst need to create their own threat actor cards?	Enexis is not familiar with the term “Threat Actor Cards”. Enexis intends to use the TIP to track individual threat actors and threat actor groups based on their TTPs, using intelligence from multiple sources. Enexis welcomes relevant examples as part of the market consultation.
36	Threat Actor Cards: Should the supplier provide a Threat Actor library that includes, IOCs, CVEs, Malware, and related sources where the Threat Actor is active in?	Enexis is not familiar with the term “Threat Actor Cards”. Enexis intends to use the TIP to track individual threat actors and threat actor groups based on their TTPs, using intelligence from multiple sources. Enexis welcomes relevant examples as part of the market consultation.
37	Timing/Planning: When is the tender expected to publish, and what’s the target start date for the contract?	Enexis has not yet determined an indicative planning. The timing of the tender and the intended contract start date will be determined following the market consultation.
38	Budget: Is there an indicative budget envelope you can share with the market?	Enexis has not yet defined an indicative budget. Through this market consultation, Enexis is seeking market input on expected costs and pricing models.
39	Aanbestedende dienst verwijst bij ‘Response tot he market consultation paper’ naar de aanbestedingstooling Mercell. Deze marktconsultatie verloopt via TenderNed. Klopt het dat het hier een verschrijving betreft?	See the answer to question 3
40	Is Enexis currently using a TIP? If so, what TIP is currently being used and what are the main reasons Enexis is looking for alternatives?	No, Enexis is currently not using a TIP
41	What Cyber Threat Intelligence sources wants Enexis to integrate in a TIP?	Enexis is looking to integrate a variaty of CTI sources in the TIP, where the TIP itself is not required to provide CTI sources but rather serve as a place to aggregate multiple sources. The exact composition of CTI sources changes over time and cannot be disclosed in a public market consultation.
42	Given that the CTI team serves both the IT-SOC and the OT-SOC with a 50/50 split, which specific OT/ICS security sources or network segments should primarily be connected to the TIP?	See the answer to question 34.
43	Are there strict requirements regarding data isolation (e.g., air-gapped components) between IT and OT threat intelligence?	Yes. A SaaS solution cannot be directly connected to the Enexis OT network. Enexis OT Architects will design propper connections if and when applicable.
44	Which specific SIEM, SOAR, and EDR solutions are currently operational within the IT and OT SOC?	See the answer to question 6.
45	Does Enexis expect the TIP to only enrich and deliver IOCs, or are you looking for a platform that can also directly execute automated blocks (enforcement) at the network and endpoint level?	Enexis expects the TIP to enrich and distribute IoCs, while also providing CTI analysts with a central workspace for their intelligence activities, such as structuring collected intelligence, creating MITRE ATT&CK mappings and tracking threat actor activity. The TIP will not be integrated in a manner that enables any form of automated enforcement.
46	Does Enexis expect the TIP to provide out-of-the-box integrations with specific Dutch or European government and sector sources (such as NCSC-NL, Z-CERT, E-ISAC, or DTC) via automated STIX/TAXII connections?	We expect the TIP to provide the capability to leverage industry standard connections and standards such as information sharing through API's, and using CTI standards suchs as the ones mentioned in the question.
47	The RFI document mentions 4 dedicated CTI analysts. Should the licensing model exclusively provide licenses for these 4 core users, or should other SOC roles (such as Detection Engineers, Threat Hunters, and Incident Responders) also receive (read-only or interactive) access to reports and dashboards?	Enexis expects the TIP to be primarily used by the four CTI analysts. However, Enexis would like to retain the flexibility to expand TIP usage to other SOC roles as the SOC and CTI functions grow and mature.
48	Should the platform provide a natively integrated SOAR orchestration engine that allows threat intelligence (IOCs) to be automatically actioned, such as performing a real-time hunt, blocking a malicious IP across firewalls, or isolating an endpoint, directly from the intelligence interface without requiring a separate third-party automation tool or manual context switching?	See the answer to question 34.

49	You are referring to an integration with MISP. Is the plan of Enexis to use MISP open source TIP platform alongside the new to be selected TIP? Or is there another reason to integrate with MISP from your perspective?	There is no formal CTI architecture defined yet.However, given the wide-spread usage of MISP within the industry, we expect the need to connect with MISP deployments in some form. This could be either downstream or upstream.
50	Your CTI team consists of 4 analysts covering both the IT-SOC and OT-SOC. Given the industry-wide shortage of specialized CTI talent, how are you evaluating the ROI of a Threat Intelligence Platform in terms of reducing external consulting/MSSP reliance and preventing analyst burnout?	Enexis does not see the relevance of this question in relation to this market consultation.
51	How does your CTI workflow handle non-technical threat data, such as PDF threat actor writeups, NCSC bulletins, or dark web intel, and how do you automatically extract and map those adversary TTPs to STIX 2.1 object structures?	Enexis' CTI workflow includes non-technical threat intelligence from various sources. Currently, the processing and mapping of this information is largely manual. Enexis expects the future TIP to support CTI analysts by providing automation capabilities for these activities.
52	How do your analysts currently correlate IT-centric indicators (e.g., email phishing hashes, C2 IPs) with OT-specific telemetry (e.g., Modbus/IEC 60870-5-104 anomalies or Claroty/Nozomi asset alerts) without having to switch between multiple management consoles?	Enexis currently operates separate SOCs for IT and OT, each with its respective focus.
53	The consultation document states 11-11-2026 as the deadline for written responses (via Mercell), while the TenderNed notice states 04-11-2026 (via TenderNed). Could Enexis confirm the applicable deadline and submission channel?	See the answer to question 2 & 3
54	Could Enexis clarify whether a fully integrated, single-vendor Threat Intelligence Platform is preferred, or whether a solution combining a central TIP with third-party intelligence services and integrations would also be acceptable? Are responses from partnerships (e.g. a threat intelligence provider together with a TIP vendor) welcome?	Enexis currently envisages a solution architecture with a separate TIP and separate Threat Intelligence providers. Enexis welcomes market feedback on this approach, but requires sufficient flexibility to avoid vendor lock-in between the TIP and the Threat Intelligence providers. Enexis must be able to switch or add Threat Intelligence providers without having to replace the TIP. The TIP should therefore support integration with both IT- and OT-specific Threat Intelligence providers.
55	Is the expected tender scope limited to the platform, or may it also include threat intelligence content (feeds, reporting) – for example as a separate lot?	See the answer to question 54.
56	Which capabilities of the intelligence lifecycle are considered mandatory within the central platform, and which may be delivered through integrations with existing tooling?	The target architecture for IOC distribution has not been defined yet. The TIP should be able to aggregate and manage IoCs and provide a consolidated IoC feed to MISP. Other parts of the intelligence lifecycle, particularly non-technical activities such as analysing intelligence reports and creating CTI products, are expected to be supported within the TIP itself.
57	Which SIEM, SOAR, TIP, XDR and other security platforms are currently used by the IT-SOC and OT-SOC, which integrations are expected to be mandatory, and are there platforms the TIP is expected to complement rather than replace?	See the answer to question 6.
58	Which external threat intelligence providers and feeds are currently used, and which must be supported from the start of the contract?	See the answer to question 41.
59	Does Enexis require bidirectional MISP integration, including synchronisation of indicators, events, relationships and associated metadata, or is one-way ingestion sufficient?	Enexis expects bi-directional integration to be required at some point.
60	Could Enexis describe its current use of MISP, including the deployment model (self-hosted or hosted), the role MISP plays in the CTI workflow, the main communities and sharing groups it is connected to (e.g. sector ISACs or national CERTs), approximate data volumes, and whether MISP is expected to remain in use alongside the future TIP or to be replaced by it?	Enexis cannot share this level of details on its current threat intelligence architecture in an open market consultation.
61	Which specific CTI use cases are required for the OT-SOC (including ICS- and energy-sector-specific intelligence), and are there restrictions concerning connectivity, data exchange or integration with operational technology environments?	Enexis requires the TIP to support integration with an OT-specific Threat Intelligence provider. For the connectivity, data exchange and integration requirements concerning the OT environment, see the answer to question 43.
62	What level of automated deduplication, correlation, source attribution and analyst-controlled merging is expected across intelligence from different providers?	Enexis aims to automate these activities to the greatest extent possible, while maintaining appropriate analyst oversight and control.
63	Which requirements apply to data residency, data processing locations, confidentiality markings, access control and sharing of intelligence with external services?	See the answer to question 8. In addition, Enexis uses TLP for confidentiality markings.
64	Is Enexis primarily looking for a self-service platform operated by its four CTI analysts, or are implementation assistance, managed services and ongoing specialist support also within scope?	Enexis is primarily looking for a self-service platform, including initial user training. Information on additional implementation, managed and specialist support services is welcome.
65	How does Enexis view the involvement of external threat intelligence specialists, including on-demand expert support, to complement and strengthen its internal CTI team?	Enexis cannot share the current state of external CTI involvement in an open market consultation. However, Enexis welcomes market input on the available options and approach.
66	Could Enexis provide indicative volumes for intelligence sources, indicators, API requests, integrations and expected data retention, to support a comparable pricing estimate?	See the answer to question 41. Indicative volumes for data retention and API requests have not yet been defined.
67	Does Enexis have an indicative budget range for the TIP solution (excluding internal FTE costs, threat intelligence feeds, integrations and other committed expenditure), a preferred contract duration and an expected implementation timeline?	Enexis has not yet determined an indicative budget range, preferred contract duration or expected implementation timeline. One of the objectives of this market consultation is to obtain market insights on these aspects to support Enexis in further defining its requirements and approach.
68	How are malware investigations and analyses currently conducted within the IT-SOC and OT-SOC, and which tools and capabilities are used to support these activities in relation to the TIP?	Malware investigation is done as part of the incident response proces. Enexis determines the relevance of tools to this proces as an investigation evolves. The CTI team aims to support this proces as much as possible.
69	What are the intelligence reporting needs and expectations at a strategic level, particularly for stakeholders such as the CIO, CISO and Line of Business management?	The Threat Intelligence tender focuses on tooling that supports the Enexis CTI team in creating tactical and operational threat intelligence. Strategic stakeholders, such as the CIO and CISO, are not expected to directly consume these CTI products. Instead, the CTI team provides these stakeholders with a quarterly update on the security landscape.
70	Which functionalities or capabilities are currently missing or considered insufficient in Enexis' existing threat intelligence set-up, and what are the main challenges the CTI team experiences in its daily workflow (e.g. working across multiple tools, portals and dashboards)?	The CTI team currently has no single pane of glass and limited automation capabilities.
71	What requirements and preferences does Enexis have regarding digital autonomy, technological sovereignty and the selection of technology partners, and to what extent do these influence its procurement and technology strategy?	Enexis considers digital autonomy and technological sovereignty within the context of applicable laws and regulations and its internal policies. Specific requirements regarding these aspects and the selection of technology partners have not yet been defined.
72	In vraag 14 refereert u aan de inkoopvoorwaarden. De opgegeven link werkt echter niet. Kunt u de juiste link naar de inkoopvoorwaarden delen?	Hereby the correct link: https://www.enexisgroep.com/media/r1vpeasl/enexis-purchasing-conditions-2025.pdf