Forumadvies versiewijziging STIX en TAXII

Vergadering:	Forum Standaardisatie
Agendapunt:	2A
Documentnummer:	20260408
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	27 maart 2026
Bijlagen:	Intakeadvies STIX en TAXII versie 2.1 Expertadvies STIX en TAXII versie 2.1
Rechten	CC0 publieke domein verklaring

1 Advies

Het Forum Standaardisatie adviseert om Structured Threat Information Expression (STIX) en Trusted Automated eXchange of Indicator Information (TAXII) in de nieuwe versie (2.1) te blijven verplichten aan de overheid via plaatsing op de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie.

Het huidige functioneel toepassingsgebied voor STIX en TAXII is:

> *STIX 1.2.1 en TAXII 1.1.1 moeten worden toegepast op de gestructureerde uitwisseling van informatie over digitale dreigingen tegen informatiesystemen.*

Het voorgestelde functioneel toepassingsgebied voor STIX en TAXII 2.1 is:

> *STIX en TAXII moeten worden toegepast op verstrekken en/of verkrijgen van informatie over cyberdreigingen tegen netwerk- en informatiesystemen.*

Het Forum Standaardisatie adviseert het functioneel toepassingsgebied te wijzigen. Het originele toepassingsgebied bood een goede basis, maar moet worden verduidelijkt en geactualiseerd. Het begrip 'uitwisselen' is gewijzigd naar 'verstrekken en/of verkrijgen', omdat 'uitwisselen' als wederzijdse communicatie kan worden opgevat, terwijl dat niet strikt noodzakelijk is. Verdere wijzigingen zijn doorgevoerd om het functioneel toepassingsgebied beter aan te laten sluiten bij de huidige wetgeving en het hedendaagse taalgebruik.

STIX en TAXII – doorgaans in combinatie gebruikt – gelden binnen de markt voor cyberindringingsdetectie en cyberdreigingsinformatie in versie 2.1 als de toonaangevende standaarden. In de rest van het Forumadvies wordt de term 'dreigingsinformatie' of 'dreigingen' gehanteerd, omdat hiermee, conform de terminologie in de Cyberbeveiligingswet (Cbw), cyberdreigingsinformatie wordt bedoeld.

Op de 'Pas toe of leg uit'-lijst staan deze standaarden onder één registratie opgenomen (STIX versie 1.2.1 en TAXII versie 1.1.1). In het Forumadvies worden STIX versie 2.1 en TAXII versie 2.1 gezamenlijk aangeduid als 'STIX en TAXII versie 2.1' en 'de standaarden'. De Organization for the Advancement of Structured Information Standards (OASIS) ontwikkelt en beheert de standaarden als onafhankelijke non-profit standaardisatieorganisatie die zich richt op de ontwikkeling en adoptie van open standaarden voor informatie-uitwisseling.

In de rest van dit document wordt dit advies nader onderbouwd. Hoofdstuk 2 geeft een korte uitleg van het nut en belang van de standaard. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam, alsmede de vervolgstappen. Hoofdstuk 4 beschrijft de resultaten van de toetsing van de standaard op de inhoudelijke hoofdcriteria. Tot slot geeft hoofdstuk 5 aanvullende adviezen om de adoptie van de standaard te stimuleren.

2 Korte beschrijving van de standaard

2.1 Over de standaard

Structured Threat Information Expression versie 2.1 (STIX versie 2.1) biedt een datamodel om informatie over dreigingen uit te wisselen op een manier die zowel mensen als machines kunnen begrijpen. Daarmee draagt de standaard bij aan het consistent verkrijgen, opslaan, analyseren en verstrekken van dreigingsinformatie. STIX versie 2.1 is relevant voor iedereen die betrokken is bij cyberweerbaarheid van organisaties, entiteiten, diens leveranciers en voor gemeenschappen die dreigingsinformatie verkrijgen en verstrekken.

Trusted Automated eXchange of Indicator Information versie 2.1 (TAXII versie 2.1) biedt een toepassingsprotocol voor het verkrijgen en verstrekken van dreigingsinformatie op een eenvoudige en schaalbare manier. TAXII versie 2.1 definieert concepten, protocollen en berichten om informatie uit te wisselen voor de detectie, preventie en beperking van dreigingen. TAXII versie 2.1 draagt bij aan het geautomatiseerd en real-time verkrijgen en verstrekken van dreigingsinformatie en stelt organisaties in staat om zicht te krijgen op komende dreigingen. Ook stelt het organisaties in staat om de informatie gemakkelijk te verkrijgen en te verstrekken met partners. TAXII is speciaal ontworpen om de uitwisseling van dreigingsinformatie te ondersteunen die in STIX wordt vertegenwoordigd. Ondersteuning voor het verkrijgen en verstrekken van STIX-content is een standaard onderdeel van TAXII versie 2.1. TAXII versie 2.1 kan echter ook worden gebruikt om gegevens in andere format te verkrijgen en verstrekken.

Het is belangrijk op te merken dat STIX en TAXII onafhankelijke standaarden zijn: de structuren en serialisaties van STIX versie 2.1 zijn niet afhankelijk van een specifiek

transportmechanisme en TAXII versie 2.1 kan worden gebruikt om niet-STIX-gegevens te transporteren.

2.2 Waarom is deze versie belangrijk?

De 'Pas toe of leg uit'-status van STIX versie 1.2.1 en TAXII versie 1.1.1 loopt achter op de dagelijkse praktijk. Veel organisaties, waaronder NCSC, gebruiken reeds versie 2.1. Ook internationaal geldt versie 2.1 als de facto versie van beide standaarden. STIX en TAXII versie 2.1 bieden ten opzichte van de vorige versies meerwaarde. De standaarden zijn verbeterd op meerdere punten ten opzichte van hun voorgaande versies.

STIX en TAXII versies 1.* waren wereldwijd veelvuldig geadopteerd en ingezet door operationele deelgemeenschappen. Voorbeelden hiervan zijn het European Union Agency for Network and Information Security (ENISA), dat bijdraagt aan cybersecurity in Europese Unie en het Forum of Incident Response and Security Teams (FIRST), dat wereldwijd samenwerkt om oplossingen te vinden voor complexe cybersecurityproblemen. Tegelijkertijd erkende de Cyber Threat Intelligence Technical Committee (CTI TC) dat deze specificaties moeilijk waren te implementeren, wat verdere adoptie bemoeilijkte. Complexe XML-structuren en te veel keuzes binnen het datamodel maakte STIX moeilijk te gebruiken. Hierdoor was het verkrijgen en verstrekken van dreigingsinformatie onnodig ingewikkeld. Daarom heeft de CTI TC voor versie 2.1 het datamodel en de opslagmethode herzien. Daarnaast is TAXII aangepast naar een eenvoudiger, Representational State Transfer (REST)-gebaseerd ontwerp. Deze verbeteringen maken STIX en TAXII versie 2.1 makkelijker te gebruiken, beter afgestemd en overzichtelijker, wat samenwerking en toepassing bevordert.

STIX versie 1.2.1 en TAXII versie 1.1.1 worden nog steeds erkend en gedocumenteerd door OASIS. Hoewel deze standaarden formeel beschikbaar blijven, richt de gemeenschap zich inmiddels op de nieuwere versies, STIX versie 2.1 en TAXII versie 2.1. Deze nieuwere versies bieden verbeterde functionaliteit en betere interoperabiliteit. De oudere 1.*-versies gelden als verouderd. Ze worden nog maar in zeer beperkte mate toegepast of ondersteund door leveranciers. Eerdere versies bevatten te veel beperkingen, wat het praktisch gebruik ervan ernstig bemoeilijkte.

Voorafgaand aan de huidige standaarden publiceerde OASIS nog de 2.0-versies, maar ook die bleken in de praktijk tekort te schieten. De verbeteringen in STIX en TAXII versie 2.1 verhelpen deze tekortkomingen. STIX en TAXII versie 2.1 ondersteunen bovendien een breed scala aan informatiesoorten. Naast dreigingen, kwetsbaarheden en incidenten beschrijven deze versies ook doelstellingen, motieven, aanvalspatronen, verdedigingstactieken en beschermingsmaatregelen.

3 Betrokkenen en proces

3.1 Gevolgde procedure

Het Nationaal Cyber Security Centrum (NCSC) heeft STIX en TAXII in de nieuwe versie (2.1) op 15 april 2025 aangemeld voor plaatsing op de 'Pas toe of leg uit'-lijst.

De procedurebegeleider InnoValor Advies heeft op 20 mei 2025 een intakegesprek gevoerd met de indiener, in aanwezigheid van Bureau Forum Standaardisatie. In dit gesprek is onderzocht of STIX en TAXII versie 2.1 voldoet aan de criteria om in procedure te worden genomen. De resultaten van het onderzoek zijn vastgelegd in het intakeadvies.

Op basis van het intakeadvies heeft het Forum Standaardisatie op 24 september 2025 besloten de standaard in procedure te nemen. Vervolgens heeft de procedurebegeleider in overleg met de indiener en Bureau Forum Standaardisatie een expertgroep samengesteld en een voorzitter aangesteld om de standaard te toetsen.

De leden van de expertgroep zijn op 8 december 2025 bijeengekomen om de standaard te toetsen aan de criteria en geïdentificeerde aandachtspunten te bespreken. Tijdens deze bijeenkomst is ook het nieuwe toepassingsgebied opgesteld. De uitkomst van het expertonderzoek is vastgelegd in het expertadvies.

Het Bureau Forum Standaardisatie publiceerde het expertadvies ter openbare consultatie via de website van Internetconsultatie van 19 januari 2026 tot 16 februari 2026. In de openbare consultatie werden geen openbare of niet-openbare reacties ontvangen.

Dit Forumadvies is opgesteld op basis van het expertadvies en inzichten van de leden van het Forum Standaardisatie. Indien het Forum Standaardisatie instemt met dit advies, wordt het aan het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) ter besluitvorming voorgelegd.

3.2 Resultaat van het expertonderzoek

De geconsulteerde experts adviseren om STIX en TAXII in de nieuwe versie (versie 2.1) te blijven verplichten aan de overheid (‘Pas toe of leg uit’) via plaatsing op de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie voor het verstrekken en/of verkrijgen van informatie over cyberdreigingen tegen netwerk- en informatiesystemen.

De experts besloten te adviseren het functioneel toepassingsgebied te wijzigen, omdat het originele toepassingsgebied weliswaar een goede basis bood, maar dat het moet worden verduidelijkt en geactualiseerd. Het begrip ‘uitwisselen’ is gewijzigd in ‘verstrekken en/of verkrijgen’, omdat ‘uitwisselen’ als wederzijdse communicatie kan worden opgevat, terwijl dat niet strikt noodzakelijk is. Verdere wijzigingen zijn doorgevoerd om het functioneel toepassingsgebied beter aan te laten sluiten bij de huidige wetgeving en het hedendaagse taalgebruik.

Het huidige functioneel toepassingsgebied voor STIX en TAXII is:

> *STIX 1.2.1 en TAXII 1.1.1 moeten worden toegepast op de gestructureerde uitwisseling van informatie over digitale dreigingen tegen informatiesystemen.*

De experts adviseren het functioneel toepassingsgebied te wijzigen naar:

> *STIX en TAXII moeten worden toegepast op verstrekken en/of verkrijgen van informatie over cyberdreigingen tegen netwerk- en informatiesystemen.*

Ook is tijdens het expertonderzoek aandacht besteed aan de beperkte adoptie van STIX en TAXII bij provincies, gemeenten en waterschappen, zoals bijvoorbeeld is gebleken uit de Evaluatie cluster 'Veilig Internet'. Dit blijft nog steeds het geval, al is wel enige verbetering zichtbaar. De provincies zijn bezig met een traject richting de inrichting van een Security Operations Center (SOC). Bij de gemeenten verloopt de adoptie goed, maar het daadwerkelijke gebruik blijft nog achter. Namens de waterschappen was geen vertegenwoordiger aanwezig bij de expertbijeenkomst. CERT-WM, het gezamenlijke cybersecurityteam van de Nederlandse waterschappen, is geattendeerd op de start van de openbare consultatie op Internetconsultatie.nl om een reactie te geven, maar er is geen reactie ontvangen.

Het NCSC heeft aangegeven de regierol op zich te willen nemen om toe te zien op het bevorderen van de adoptie van de standaard in Nederland en te fungeren als vertegenwoordiger van de Nederlandse gebruikers naar de internationale beheerorganisatie.

De experts adviseren het Forum Standaardisatie om het NCSC formeel te benaderen met het verzoek deze regierol daadwerkelijk op zich te nemen. Als onderdeel van deze toegezegde regierol functioneert het NCSC als nationale vertegenwoordiger en richt het een duidelijk en toegankelijk aanspreekpunt in voor informatie, ondersteuning en documentatie over STIX en TAXII versie 2.1.

Ook adviseren de experts het NCSC een actieve rol op zich te nemen binnen de Technical Committee (TC) van OASIS, bij voorkeur ook met vertegenwoordiging in het bestuur.

Verder adviseren de experts dat het NCSC het belang van systemen voor interoperabiliteitschecks nadrukkelijker onder de aandacht brengt bij de beheerorganisatie OASIS en het finaliseren van bestaande drafts hiervoor aanmoedigt.

Tot slot adviseren de experts het Forum Standaardisatie om na aanmelding van een nieuwe versie van de standaarden te toetsen of het NCSC voldoet aan de criteria voor het predicaat 'Uitstekend beheer' voor Nederlandse intermediair (Erkend Nederlands Intermediair), als het NCSC heeft aangegeven de regierol volwaardig te hebben opgepakt en ingevuld en voor het predicaat in aanmerking te willen komen.

3.3 Resultaat van de openbare consultatie

In de openbare consultatie werden geen openbare of niet-openbare reacties ontvangen.

4 Toetsing op inhoudelijke hoofdcriteria

Het Forum Standaardisatie hanteert vier inhoudelijke hoofdcriteria om te toetsen in hoeverre een standaard in aanmerking komt voor verplichten (‘Pas toe of leg uit’) of aanbevelen aan de overheid.

1. Heeft de standaard toegevoegde waarde?
2. Zijn de standaard en het standaardisatieproces voldoende open?
3. Heeft de standaard voldoende draagvlak?
4. Is opname op de lijst een passend middel om de adoptie te bevorderen?

Ieder van deze hoofdcriteria heeft deelcriteria die staan beschreven op de website van het Forum Standaardisatie. Dit hoofdstuk beschrijft per criterium het resultaat van de toetsing.

4.1 Toegevoegde waarde

De toetsingsprocedure wijst uit dat STIX en TAXII versie 2.1 voldoet aan het criterium ‘Toegevoegde waarde’.

De standaarden stellen organisaties in staat eenvoudiger en efficiënter dreigingsinformatie met elkaar uit te wisselen. Veel organisaties, waaronder NCSC, gebruiken reeds versie 2.1. Ook internationaal geldt versie 2.1 als de facto standaard. De standaarden zijn verbeterd op meerdere punten. De nieuwe versie van STIX en TAXII maakt het mogelijk om meer gedetailleerde en meer volledige informatie te verkrijgen en te verstrekken. Het is bijvoorbeeld mogelijk om informatie te verkrijgen en verstrekken over het gedrag van een actor. Dit was in de vorige versie nog niet mogelijk. De nieuwe versie is tevens makkelijker implementeerbaar. Het toepassen van STIX en TAXII versie 2.1 vormt op zichzelf geen beveiligingsrisico, maar een onveilige implementatie of onjuist gebruik kan wel risico’s introduceren. Mogelijke gevaren zijn het automatisch verwerken van onbetrouwbare dreigingsinformatie, het onbedoeld verkrijgen en verstrekken van gevoelige data, een verkeerde inrichting van de toegangsbeveiliging van TAXII-endpoints (toegangspunten voor het ophalen of aanbieden van dreigingsinformatie), en overbelasting van systemen.

Wat betreft privacyrisico’s geldt dat STIX en TAXII versie 2.1 zelf geen directe risico’s veroorzaken, maar dat de inhoud van de gedeelde data risico’s met zich mee kan brengen. Wanneer STIX-objecten persoonsgevoelige gegevens bevatten zoals IP-adressen, e-mailadressen of metadata die herleidbaar zijn tot personen, kunnen privacy- of AVG-implicaties ontstaan. Het risico zit dus niet in de standaard, maar in de data die ermee wordt uitgewisseld.

STIX en TAXII versie 2.1 kunnen over de grenzen van organisaties of sectoren worden gebruikt en zijn niet alleen bedoeld voor gegevensuitwisseling binnen één organisatie of sector. Hoewel de standaarden in theorie ook kunnen worden gebruikt voor communicatie tussen overheidsorganisaties en burgers, is dit minder gebruikelijk. Dit komt doordat STIX en TAXII versie 2.1 zich richten op technische en gedetailleerde informatie over dreigingen. Juist deze mate van detail en technische specificiteit stelt organisaties met gespecialiseerde

cybersecurityafdelingen en een hoog volwassenheidsniveau in staat om dreigingsinformatie geautomatiseerd te verwerken, te analyseren en te integreren in hun securitymonitoring. Hierdoor kunnen zij dreigingen sneller detecteren, beter duiden en gerichter mitigerende maatregelen nemen.

De kosten van implementatie zijn acceptabel, omdat zonder het gebruik van deze standaarden organisaties telkens afzonderlijke afspraken moeten maken voor de uitwisseling van gestructureerde dreigingsinformatie. Het gebruik van STIX en TAXII versie 2.1 maakt deze uitwisseling efficiënter, doordat de informatie op een uniforme en machineleesbare manier beschikbaar wordt gesteld en eenvoudig geïntegreerd kan worden in systemen. Specifieke kosten voor de implementatie van STIX en TAXII versie 2.1 zijn niet bekend, omdat deze afhankelijk zijn van de gekozen implementatie.

Het NCSC heeft vanuit wetgeving de taak om organisaties binnen zijn doelgroep, waaronder Rijksoverheidsorganisaties en NIS2-organisaties, adequaat te informeren over dreigingen. Daartoe biedt het NCSC gestructureerde dreigingsinformatie aan, specifiek op het gebied van Cyber Threat Intelligence (CTI). Deze CTI-data worden momenteel aan Rijksoverheidsorganisaties beschikbaar gesteld via de open STIX en TAXII versie 2.1 standaarden. Door het gebruik van STIX en TAXII versie 2.1 ontvangen organisaties de dreigingsinformatie op een uniforme en gestructureerde manier, waardoor zij deze goed kunnen verwerken en integreren in hun eigen security monitoring-oplossingen.

Naast het gebruik van STIX en TAXII versie 2.1 maakt de Nederlandse overheid en organisaties daarbuiten veel gebruik van de open source software Malware Information Sharing Platform (MISP) als platform voor het delen en beheren van dreigingsinformatie. MISP gebruikt standaard een eigen formaat dat niet wordt beheerd door een standaardisatieorganisatie. Met additionele open source software kan informatie van MISP worden omgezet naar STIX en kan informatie uit STIX worden ingeladen in MISP. Zowel bij MISP als bij STIX zijn medewerkers van het Computer Incident Response Center Luxembourg (CIRCL) betrokken. Er wordt momenteel gewerkt aan verdere integratie van STIX in de MISP-omgeving, wat de adoptie van STIX kan versterken, zoals beschreven in de MISP-STIX Library.

4.2 Open standaardisatieproces

De toetsingsprocedure wijst uit dat het beheer van STIX en TAXII versie 2.1 voldoet aan het criterium ‘Open standaardisatieproces’.

Het specificatiedocument van STIX versie 2.1 is te vinden via de OASIS-website. Ook het specificatiedocument van TAXII versie 2.1 is vrij toegankelijk via OASIS. De documentatie over het ontwikkel- en beheerproces van STIX en TAXII versie 2.1 is publiek beschikbaar via de OASIS-website.

OASIS garandeert dat partijen die bijdragen aan de ontwikkeling van de standaarden hun intellectueel eigendomsrecht onherroepelijk royalty-free voor eenieder beschikbaar stellen. OASIS is een internationaal non-profit consortium dat zich richt op de ontwikkeling en adoptie

van open standaarden voor informatie-uitwisseling. Het besluitvormingsproces is toegankelijk voor alle belanghebbenden, waaronder gebruikers, leveranciers, adviseurs en wetenschappers. OASIS biedt hiervoor verschillende mogelijkheden. Actief bijdragen aan de ontwikkeling van de standaarden kan door deel te nemen aan de Technical Committee (TC). De financiering van de ontwikkeling en het onderhoud van de standaarden is voor ten minste drie jaar gegarandeerd.

Waar OASIS de internationale beheerfunctie vervult, kan het NCSC binnen Nederland een centrale regierol vervullen. De 'Gespreksnotitie regierol standaarden STIX TAXII in Nederland' van Forum Standaardisatie adresseert het ontbreken van een sturende rol in Nederland op de open standaarden STIX en TAXII. De gespreksnotitie benadrukt het belang van een actieve regierol van het NCSC bij het beheer en de toepassing van deze standaarden. Het Forum Standaardisatie adviseert dat het NCSC een actieve rol neemt binnen de Technical Committee (TC) van OASIS, bij voorkeur ook met vertegenwoordiging in het bestuur, zodat de Nederlandse belangen bij de ontwikkelingen rondom deze standaard voldoende worden behartigd.

Het NCSC is voornemens om vanuit deze regierol:

- de inbreng te monitoren van Nederlandse organisaties tijdens openbare consultaties en bij deelname aan publiek aangekondigde overleggen van OASIS.
- de doorontwikkeling en het beheer van de standaard door OASIS onder de aandacht te brengen in Nederland.
- te onderzoeken op welke wijze aansluiting kan worden gezocht bij OASIS als beheerder van de standaard.
- om het Nederlandse belang onder de aandacht van de beheerder te brengen.

Ook heeft het NCSC de intentie om:

- de publieke consultatie die door OASIS wordt georganiseerd actief onder de aandacht te brengen bij de Nederlandse overheid.
- tijdig relevante ontwikkelingen richting OASIS en richting Nederlandse belanghebbenden te signaleren.
- het Nederlandse belang onder de aandacht van de beheerder te brengen.
- een trekkende rol te vervullen in verschillende standaardisatieprocessen.

Daarnaast is het NCSC ervaringsdeskundige op het gebied van STIX en TAXII versie 2.1. Vanuit deze rol is het NCSC zelf ook belanghebbende: het draagt bij aan de adoptie, omdat cybersecurityinformatie met deze standaard wordt verkregen en uitgewisseld, en het brengt zijn eigen belangen in bij OASIS.

4.3 Draagvlak

De toetsingsprocedure wijst uit dat STIX en TAXII versie 2.1 voldoet aan het criterium 'Draagvlak'.

Meerdere Nederlandse overheidsorganisaties die vallen onder het organisatorisch werkingsgebied gebruiken de aangemelde versie van de standaarden. Aangezien het NCSC de standaarden toepast voor hun doelgroep, zullen andere Rijksoverheidsorganisaties deze standaarden ook hanteren. Daarnaast bieden meerdere leveranciers ondersteuning en het zijn breed geaccepteerde standaarden voor het verkrijgen en verstrekken van dreigingsinformatie. Verschillende commerciële partijen passen deze standaarden toe in hun producten. Een overzicht van commerciële en open source-implementaties is beschikbaar via de OASIS-wiki.

Het NCSC heeft deelnemers aan het Nationaal Detectie Netwerk (NDN) geïnformeerd over de standaarden. Op basis van de ontvangen feedback is de verwachting dat zij positief tegenover adoptie van de standaarden staan. Ook de sectorale CSIRTs spreken hun steun uit voor de standaarden. Uit de Evaluatie cluster 'Veilig Internet' blijkt dat gebruik bij provincies, gemeenten en waterschappen achterblijft. Dit blijft nog steeds het geval, al is wel enige verbetering zichtbaar. De provincies zitten in de voorfase van de inrichting van een Security Operations Center (SOC) en zijn daarom nog niet klaar voor gebruik van de standaarden. Wel staan ook zij positief tegenover de standaarden. Bij de gemeenten verloopt de adoptie goed, maar het daadwerkelijke gebruik blijft nog achter. Namens de waterschappen kon geen vertegenwoordiger aanwezig zijn bij de expertbijeenkomst. CERT-WM is geattendeerd op de start van de openbare consultatie op Internetconsultatie.nl om een reactie te geven, maar er is geen reactie ontvangen.

Lokale profielen zijn mogelijk, maar STIX versie 2.1 tracht dit overbodig te maken. Bij STIX 2.x is ervoor gekozen om veel eigenschappen van objecten verplicht te maken en meer eenduidigheid te creëren. Het Forum Standaardisatie is van mening dat het gebruik van lokale profielen voor STIX en TAXII versie 2.1 in de Nederlandse context niet nodig is.

4.4 Opname op de lijst bevordert adoptie

De toetsingsprocedure wijst uit dat STIX en TAXII versie 2.1 voldoet aan het criterium 'Opname op de lijst bevordert adoptie'.

Versie 1.2.1 van STIX en versie 1.1.1 van TAXII staan op de 'Pas toe of leg uit'-lijst, waardoor deze afweging eerder heeft plaatsgevonden. Opname verhoogt de bekendheid en daarmee de adoptie van de standaard door organisaties. De nieuwe versies van STIX en TAXII maakt het relevant om de status 'Pas toe of leg uit' bij het Forum Standaardisatie te behouden. In de praktijk adviseert het NCSC inmiddels het gebruik van STIX en TAXII versie 2.1 bij de aanschaf van nieuwe cybersecuritysoftware, wat niet in lijn is met de versie die momenteel op de lijst staat.

Het NCSC geeft invulling aan zijn rol voor het verkrijgen en verstrekken van dreigingsinformatie door gebruik te maken van deze standaarden. Het NCSC kan voor verdere adoptie van STIX en TAXII versie 2.1 een actieve regierol binnen het stelsel vervullen. Door tijdige aanmeldingen van nieuwe versies om de registratie actueel te houden op de lijst van Forum Standaardisatie, contact te onderhouden met OASIS en internationale

ontwikkelingen te vertalen naar de Nederlandse context, kan het NCSC een belangrijke bijdrage leveren aan het breder gebruik van de standaarden binnen Nederland. Ook de sectorale CSIRTs zien de meerwaarde van de standaarden en opname op de lijst.

5 Adviezen bij opname van de standaard

Het Forum Standaardisatie geeft het OBDO meerdere adviezen bij opname van versie 2.1 van STIX en TAXII op de 'Pas toe of leg uit'-lijst. Indien NCSC voldoet aan de aan hem gerichte adviezen, geeft het daarmee invulling aan de criteria voor het verkrijgen van het predicaat 'Uitstekend beheer' voor Nederlandse intermediair (Erkend Nederlands Intermediair) en geeft het opvolging aan de gestelde adoptieadviezen bij de plaatsing van STIX en TAXII eind 2017 op de 'Pas toe of leg uit'-lijst. Het Forum Standaardisatie kan in een later stadium toetsen of het NCSC daadwerkelijk voldoet aan deze criteria.

Hieronder volgen de gegeven adviezen plus een verwijzing naar de criteria voor Erkend Nederlands Intermediair en de eerder gestelde adoptieadviezen uit 2017 (tevens hieronder uitgeschreven).

5.1 Adviezen bij opname versie 2.1 STIX en TAXII

1. Het Forum Standaardisatie adviseert het NCSC om, als onderdeel van de toegezegde regierol, te functioneren als nationale vertegenwoordiger en een duidelijk en toegankelijk aanspreekpunt in te richten voor informatie, ondersteuning en documentatie over STIX en TAXII versie 2.1.

➔ Geeft invulling aan adoptieadviezen 2017 (1), (2), (3) en (4)

➔ Geeft invulling aan criteria Erkend Nederlands Intermediair (1), (2) en (3) (= alle criteria)

2. Het Forum Standaardisatie adviseert dat het NCSC een actieve rol op zich neemt binnen de Technical Committee (TC) van OASIS, bij voorkeur ook met vertegenwoordiging in het bestuur;

➔ Geeft invulling aan criterium Erkend Nederlands Intermediair (2)

3. Het Forum adviseert het NCSC om het belang van systemen voor interoperabiliteitschecks nadrukkelijker onder de aandacht te brengen bij de beheerorganisatie OASIS en het finaliseren van bestaande drafts hiervoor aan te moedigen;

➔ Geeft invulling aan criterium Erkend Nederlands Intermediair (2)

4. NCSC wordt geadviseerd het Forum Standaardisatie te verzoeken om te toetsen of het NCSC voldoet aan de criteria voor het predicaat 'Uitstekend beheer' voor Nederlandse intermediair (Erkend Nederlands Intermediair), zodra het NCSC de regierol volwaardig heeft ingevuld.

➔ Geeft invulling aan adoptieadviezen 2017 (1), (2), (3) en (4)

➔ Geeft invulling aan criteria Erkend Nederlands Intermediair (1), (2) en (3) (= alle criteria)

5.2 Voorwaarden voor het verkrijgen van het predicaat 'Uitstekend beheer' voor Nederlandse intermediair (Erkend Nederlands Intermediair)

Voor het verkrijgen van het predicaat 'Uitstekend beheer' voor Nederlandse intermediair (Erkend Nederlands Intermediair) gelden de voorwaarden dat de Nederlandse organisatie:

(1) in Nederland de adoptie van de standaard actief stimuleert.

(2) direct betrokken is bij de ontwikkelingen, bijvoorbeeld door een lidmaatschap van de internationale beheerorganisatie en daarmee invloed uit moeten kunnen oefenen op de standaard.

(3) zich inzet op informatieverspreiding en kennisuitwisseling.

5.3 Adviezen van 21 november 2017 bij toekenning status 'Pas toe of leg uit' aan STIX en TAXII

(1) Het Forum Standaardisatie roept het NCSC op om samen met betrokkenen een leidraad op te stellen, al dan niet als onderdeel van een bestaand kennisproduct, ten behoeve van het eenduidig gebruik van de standaarden. De toepassing van STIX en TAXII zal veel effectiever zijn als ook op het vlak van semantiek standaardisatie plaatsvindt. De leidraad moet dit borgen. Onderdeel van de leidraad dient ook te zijn dat bij het gebruik van STIX en TAXII de toepassing van CybOx wordt geadviseerd.

(2) Het Forum Standaardisatie adviseert het NCSC om mede in de context van het Nationaal Detectie Netwerk (een samenwerking van onder andere het NCSC voor het beter en sneller waarnemen van digitale gevaren en risico's) kennisbijeenkomsten te organiseren voor het verspreiden van kennis over en ervaring met het gebruik van STIX en TAXII.

(3) Het Forum Standaardisatie roept betrokkenen bij SOC's (security operations centres) en CERT's (computer emergency response teams) binnen de overheid en publieke sector op om kennis op te doen over de meerwaarde en toepassing van de uitwisseling van gestructureerde dreigingsinformatie met STIX en TAXII.

(4) Het Forum Standaardisatie roept overheden die STIX en TAXII toepassen op om informatie over de meerwaarde van het gebruik voor hen en best practices te delen.

(5) Het Forum Standaardisatie roept VNG op om in de GGI (gemeentelijke gemeenschappelijke infrastructuur) STIX en TAXII toe te passen in het SOC (security operations center).