Expertadvies versiewijziging STIX en TAXII

Aan:	Forum Standaardisatie
Van:	Innovalor Advies B.V.
Datum:	19 januari 2026
Versie:	1.0
Bijlagen:	geen

1 Advies

De experts die betrokken waren bij het expertonderzoek adviseren 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.*

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.*

De experts hebben besloten te adviseren het functioneel toepassingsgebied te wijzigen, naar aanleiding van een voorstel van de indiener bij het intakeadvies. De experts waren van mening dat het originele toepassingsgebied 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.

Deze standaarden 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 expertadvies 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 expertadvies worden STIX versie 2.1 en TAXII versie 2.1 gezamenlijk aangeduid als 'STIX en TAXII versie 2.1' en 'de standaarden'. 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.

Tijdens de expertbijeenkomst en het tot stand komen van het expertadvies is extra aandacht besteed aan de volgende punten:

- Aandacht voor de beschrijving van het functioneel toepassingsgebied door de indiener NCSC;
- Aandacht voor mogelijke wetgeving die verplichtingen oplegt voor het verkrijgen en verstrekken van cyber security informatie;
- Aandacht voor de maatschappelijke waarde van de standaard;
- Aandacht voor de regierol van het NCSC bij het beheer en de toepassing van STIX en TAXII versie 2.1 in Nederland;
- Aandacht voor de toepassing van STIX en TAXII versie 2.1 bij gemeenten en waterschappen.

In de rest van dit document wordt dit advies nader onderbouwd. Hoofdstuk 2 geeft een korte beschrijving van het nut en belang van de standaard. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam, alsmede de vervolgstappen. Hoofdstuk 4 geeft de samenstelling van de expertgroep weer. Hoofdstuk 5 documenteert hoe de experts de standaard beoordelen tegen de criteria voor opname op de lijst. Tot slot geeft hoofdstuk 6 aanvullende adviezen van de experts aan het Forum Standaardisatie en het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) 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 standaard belangrijk?

2.2.1 Waarom zijn STIX en TAXII belangrijk?

Mede door toenemende cyberdreigingen is er steeds meer aandacht voor de digitale weerbaarheid van organisaties. Kennis over actuele cyberdreigingen is hierbij essentieel. STIX heeft een belangrijke rol voor goede informatie-uitwisseling van dreigingsinformatie. Het biedt een consistent, gestructureerd en machineleesbaar formaat om indicatoren, incidenten en dreigingsactoren eenduidig te beschrijven, verkrijgen en verstrekken. TAXII is ontworpen om ook de uitwisseling te ondersteunen van dreigingsinformatie die in STIX wordt vertegenwoordigd. Door deze standaarden gezamenlijk toe te passen, kunnen organisaties informatie over dreigingen verkrijgen en verstrekken. Dit verhoogt de cyberveiligheid en digitale weerbaarheid van de overheid en instellingen in de (semi-)publieke sector maar ook private sectoren. Opname op de lijst stimuleert de verdere adoptie van deze standaarden voor het geautomatiseerd verkrijgen en verstrekken van dreigingsinformatie (binnen de overheid).

Digitale dreigingen en aanvallen treffen steeds meer organisaties. De Nederlandse Cybersecuritystrategie van 2022-2028 bevestigt dit beeld: “De digitale dreiging is permanent en neemt eerder toe dan af, met alle mogelijke gevolgen van dien.”. Een van de uitdagingen met betrekking tot de digitale weerbaarheid is dat de afgelopen jaren is gebleken dat informatie-uitwisseling is gefragmenteerd, waardoor dreigingsinformatie niet altijd alle organisaties tijdig heeft bereikt en in staat heeft gesteld om maatregelen te treffen. Een goed werkende en snelle informatie-uitwisseling is in deze situatie cruciaal. De NIS2 richtlijn benadrukt daarbij het belang van gestandaardiseerde informatie-uitwisseling. De Cyberbeveiligingswet (Cbw), die de Wet beveiliging netwerk- en informatiesystemen (Wbni) vervangt en de NIS2 richtlijn nationaal implementeert, verplicht organisaties en bedrijven om cybersecurityinformatie uit te wisselen. Voor sectoren waar de Cbw niet geldt geeft de Wet bevordering digitale weerbaarheid bedrijven (Wbdwb) organisaties het mandaat om informatie over dreigingen uit te wisselen. Door deze wettelijke verplichtingen en mandaten zal er meer dreigingsinformatie worden gedeeld. Zonder standaardisatie kan deze informatie

niet effectief en tijdig worden gebruikt om dreigingen te detecteren. Dit benadrukt het belang van uniforme standaarden voor een effectieve en veilige informatie-uitwisseling.

2.2.2 Waarom is de nieuwe 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 cybersecurity problemen. 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

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

Op 20 mei 2025 heeft een intakegesprek plaatsgevonden met de indiener, de procedurebegeleider en Bureau Forum Standaardisatie. In dit gesprek is verkend 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 dit intakeadvies heeft het Forum Standaardisatie op 24 september 2025 besloten de aanmelding 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 in een expertsessie nader te bespreken.

Voorafgaand aan de expertbijeenkomst hebben de leden van de expertgroep een concept-expertadvies gekregen dat is samengesteld met informatie uit de aanmelding en het intake-onderzoek.

De leden van de expertgroep zijn op 8 december 2025 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook het functioneel toepassingsgebied en het organisatorisch werkingsgebied vastgesteld. Door een gebrek aan tijd kon tijdens de bijeenkomst niet het volledige expertadvies worden besproken. De experts hebben daarom hun bevindingen met betrekking tot hoofdstuk 5.4 (Opname op de lijst bevordert adoptie) schriftelijk aangeleverd. De adoptieadviezen uit hoofdstuk 6 (Adviezen bij opname van de standaard) zijn tijdens de bijeenkomst verzameld en aanvullende adviezen zijn schriftelijk aangeleverd. Dit expertadvies geeft de uitkomst van de expertsessie weer.

Het Bureau Forum Standaardisatie publiceert dit expertadvies ter openbare consultatie via de website van Internetconsultatie. Gedurende de consultatieperiode kan iedereen op het expertadvies reageren.

Na afsluiting van de openbare consultatie ontvangt de indiener een terugkoppeling op de reactie(s). Indien nodig kan dit aanleiding geven tot een aanvullend expertonderzoek.

Het Forum Standaardisatie formuleert op basis van het expertadvies, de reactie(s) uit de openbare consultatie en inzichten van de leden van het Forum Standaardisatie zelf een advies aan het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO). Het OBDO besluit om het advies wel of niet over te nemen.

4 Samenstelling van de expertgroep

Forum Standaardisatie streeft naar een samenstelling van de expertgroep met een evenwichtige publiek-private vertegenwoordiging van (toekomstige) gebruikers, leveranciers, wetenschappers en andere belanghebbenden. De expertgroep heeft een onafhankelijk voorzitter die de expertbijeenkomst leidt.

Aan de expertsessie hebben de volgende personen deelgenomen:

- Luitzen Homma (NCSC - Indiener)

- Daan Willems (NCSC - Indiener)
- Joost Altena (RDI)
- Jeroen de Baare (UWV)
- Aukjan van Belkum (Pandora Intelligence)
- Albert Welboren-Groen (CISO Rijk)
- Jan Husselson (Capgemini)
- Melvin Koelewijn (SURF)
- Twan van der Meer (IBD)
- Reshma Pandohi Mishre (CIBO)
- Gijs Rijnders (Politie)
- Patrick Tang (DICTU)

Als onafhankelijk voorzitter is opgetreden Ruud Kosman, Managing Partner bij InnoValor Advies. Aday Destici, Projectondersteuner en Koen de Jong, Adviseur bij InnoValor Advies, hebben de procedure in opdracht van het Bureau Forum Standaardisatie begeleid.

Bart Knubben, Wouter Kobes en Joram Verspaget van het Bureau Forum Standaardisatie waren als toehoorder bij de expertbijeenkomst aanwezig.

5 Toetsing op inhoudelijke criteria

Het Forum Standaardisatie hanteert vier hoofdcriteria om te bepalen of een standaard in aanmerking komt voor verplichten aan de overheid (‘Pas toe of leg uit’-verplichting) via plaatsing op de 'Pas toe of leg uit'-lijst van Forum Standaardisatie:

1. Heeft de standaard toegevoegde waarde?
2. Zijn de standaard en het standaardisatieproces voldoende open?
3. Heeft de standaard voldoende draagvlak?
4. Bevordert opname van de standaard op de ‘Pas toe of leg uit’-lijst de adoptie?

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

5.1 Toegevoegde waarde

Met dit criterium wordt bepaald of het toepassingsgebied van de standaard duidelijk is, of deze zich goed verhoudt tot andere standaarden die al dan niet op de lijst staan, of de standaard een duidelijke meerwaarde heeft en of deze opweegt tegen eventuele risico’s en nadelen.

5.1.1 Waardering van het criterium criteria ‘Toegevoegde waarde’

De experts komen tot de conclusie dat STIX en TAXII versie 2.1 voldoen aan het criterium ‘toegevoegde waarde’. Deze conclusie wordt in de volgende paragrafen toegelicht.

5.1.2 Is het toepassings- en werkingsgebied van de aanmelding goed gedefinieerd?

5.1.2.1 Is het functioneel toepassingsgebied goed gedefinieerd?

Het voorgestelde functioneel toepassingsgebied voor STIX en TAXII versie 2.1 op de 'Pas toe of leg uit'-lijst is:

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

De experts oordelen dat dit functioneel toepassingsgebied voldoende duidelijk is en het verplichte gebruik van de standaard eenduidig beschrijft.

De experts hebben besloten te adviseren het functioneel toepassingsgebied te wijzigen, naar aanleiding van een voorstel van de indiener bij het intakeadvies. De experts waren van mening dat het originele toepassingsgebied een goede basis bood, maar dat het moest 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.

5.1.2.2 Is het organisatorisch werkingsgebied goed gedefinieerd?

Het organisatorisch werkingsgebied voor STIX en TAXII versie 2.1 op de 'Pas toe of leg uit'-lijst is:

> *Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.*

Dit is het gangbare organisatorisch werkingsgebied voor standaarden op de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie.

Het geformuleerde organisatorisch werkingsgebied van de standaard is voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid. De functionele toepassing van de standaard overstijgt het organisatorisch werkingsgebied van een enkele organisatie of sector.

5.1.2.3 Is de standaard generiek toepasbaar (en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke organisaties)?

Ja, de standaard kan over de grenzen van organisaties of sectoren gebruikt worden en is 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. Deze

informatie is vooral relevant voor organisaties met gespecialiseerde securityafdeling(en) met een hoog volwassenheidsniveau.

5.1.3 Verhoudt de standaard zich goed tot andere standaarden?

5.1.3.1 Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast?

Ja, de experts stellen vast dat de standaard kan worden gebruikt met de reeds opgenomen standaarden op de lijst. De standaarden maken bijvoorbeeld gebruik van JSON.

5.1.3.2 Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied?

Niet van toepassing. De experts stellen vast dat er geen standaarden op de lijst staan met een overlappend functioneel toepassingsgebied.

5.1.3.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname?

Niet van toepassing. De experts zien geen concurrerende open standaarden die in aanmerking zou kunnen komen voor opname op de 'Pas toe of leg uit-lijst.

5.1.3.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden?

Ja, de standaard is een internationale standaard die is uitgegeven door Organization for the Advancement of Structured Information Standards (OASIS). Een internationale non-profit consortium dat zich richt op de ontwikkeling en adoptie van open standaarden voor informatie-uitwisseling.

5.1.4 Wegen de voordelen van de standaard op tegen de nadelen?

5.1.4.1 Zijn de kosten van implementatie acceptabel en zijn deze kosten bekend en inzichtelijk?

Ja, zonder gebruik van deze standaarden moeten steeds aparte afspraken worden gemaakt voor de uitwisseling van gestructureerde dreigingsinformatie. Het gebruik van STIX en TAXII versie 2.1 is daardoor efficiënter. Specifieke kosten van implementatie van STIX en TAXII versie zijn niet bekend. De experts geven aan dat deze afhankelijk zijn van de gekozen implementatie.

5.1.4.2 Is er een (kwalitatieve) businesscase van de standaard aanwezig?

Ja, de aanwezige sectorale CSIRTs zien allen een businesscase. Als voorbeeld wordt de businesscase voor gebruik door het NCSC en haar partners beschreven.

Het NCSC heeft vanuit wetgeving de taak om organisaties binnen haar 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, zoals een Threat Intelligence Platform (TIP), Security Information and Event Management (SIEM), Extended Detection and Response (XDR) of Network Detection and Response (NDR). Door deze integratie kunnen organisaties gericht monitoren of specifieke dreigingen zich manifesteren binnen hun eigen omgeving. Daarnaast kunnen doelgroeporganisaties van het NCSC vanaf 2026 automatisch waargenomen dreigingen, zogenaamde sightings, rapporteren aan het NCSC. Dit gebeurt via dezelfde STIX en TAXII versie 2.1 standaarden. Hierdoor ontvangt het NCSC signalen van dreigingen vanuit meerdere organisaties, wat bijdraagt aan een versterkt en actueel dreigingsbeeld voor Nederland. Deze aanpak bouwt voort op het bestaande Nationaal Detectie Netwerk (NDN). Het nieuwe uitwisselingsconcept op basis van STIX en TAXII versie 2.1 is reeds getest via een pilotfase, een private preview en een public review.

5.1.4.3 Is de meerwaarde van de standaard goed inzichtelijk te maken?

Ja, de standaard stelt 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 maakt het mogelijk om gedetailleerdere en volledigere informatie te verkrijgen en 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.

5.1.4.4 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Ja, STIX en TAXII versie 2.1 vormen op zichzelf geen beveiligingsrisico, maar een onveilige implementatie of onjuist gebruik kan wel risico's introduceren. De beveiligingsrisico's zijn niet veranderd ten opzichte van de vorige versie van de standaarden.

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. Organisaties kunnen deze risico's goed beheersen door betrouwbare bronnen voor dreigingsinformatie te gebruiken, goed toegangs- en autorisatiebeleid, gegevens zorgvuldig te controleren en regelmatig testen op kwetsbaarheden uit te voeren.

Met een correcte implementatie biedt STIX en TAXII versie 2.1 een veilig en waardevol instrument voor gestructureerde dreigingsinformatie-uitwisseling. De beveiligingsrisico's hebben vooral betrekking op beveiligingsstandaarden die organisaties in combinatie met STIX en TAXII toepassen.

5.1.4.5 Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Ja, 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 persoonsgegevens 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. Dit is opgenomen in de privacy considerations van STIX. De privacyrisico's zijn niet veranderd ten opzichte van de vorige versie van de standaarden.

5.2 Open standaardisatieproces

Met dit criterium wordt bepaald of het beheer en de (door)ontwikkeling van de standaard op een open, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze zijn ingericht.

5.2.1 Waardering van het criterium criteria 'Open standaardisatieproces'

De experts komen tot de conclusie dat STIX en TAXII versie 2.1 voldoen aan het criterium 'Open standaardisatieproces'. Deze conclusie wordt in de volgende paragrafen toegelicht.

Experts adviseren het NCSC om actief de regierol voor de standaarden in te vullen, om als nationale vertegenwoordiger te functioneren en een duidelijk en toegankelijk aanspreekpunt in te richten voor informatie, ondersteuning en documentatie over STIX en TAXII versie 2.1. Experts spreken het vertrouwen uit dat het NCSC de regierol naar behoren kan invullen. Anderzijds constateren zij dat het NCSC nog niet aan de gestelde voorwaarden voldoet om het predicaat 'Uitstekend beheer' toegewezen te krijgen. De experts adviseren het Forum Standaardisatie om een expertbijeenkomst te organiseren om te toetsen of het NCSC voldoet aan de criteria voor het predicaat 'Uitstekend beheer' voor Nederlandse intermediair (Erkend Nederlands Intermediair) zodra NCSC de regierol heeft ingevuld.

5.2.2 Is de documentatie voor eenieder drempelvrij beschikbaar?

5.2.2.1 Is het specificatiedocument zonder belemmeringen beschikbaar?

Ja, de documentatie van de standaarden zijn publiek en zonder onacceptabele belemmeringen beschikbaar. 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.

5.2.2.2 Is de documentatie over het ontwikkel- en beheerproces beschikbaar zonder dat er sprake is van belemmeringen?

Ja, de documentatie over het ontwikkel- en beheerproces van STIX en TAXII versie 2.1 is publiek beschikbaar via de OASIS-website.

5.2.3 Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is?

5.2.3.1 Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard onherroepelijk royalty-free voor eenieder beschikbaar?

Ja, de standaarden zijn vrij implementeerbaar en te gebruiken. Het betreft een open standaard. OASIS, de standaardisatieorganisatie, stelt het intellectuele eigendomsrecht met betrekking tot de standaard onherroepelijk royalty-free voor eenieder beschikbaar.

5.2.3.2 Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht voor (onderdelen van) de standaard onherroepelijk royalty-free voor eenieder beschikbaar stellen?

Ja, de standaardisatieorganisatie 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. OASIS ontwikkelt standaarden die bijdragen aan interoperabiliteit en samenwerking tussen verschillende systemen en organisaties.

5.2.4 Is de inspraak van eenieder in voldoende mate geborgd?

5.2.4.1 Is het besluitvormingsproces toegankelijk voor alle belanghebbenden?

Ja, 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). Hiervoor is lidmaatschap van OASIS vereist. De lidmaatschapskosten van de standaardisatieorganisatie variëren afhankelijk van de grootte van de organisatie en het type lidmaatschap: van €1.800 per jaar voor contributors zoals kleine overheden, tot €70.000 per jaar voor premium sponsors. Via het lidmaatschap dragen organisaties actief bij aan het standaardisatieproces. Naast lidmaatschap kunnen bedrijven en organisaties ook specifieke projecten of werkgroepen sponsoren, wat bijdraagt aan de financiering van de activiteiten van OASIS. De financiering van de ontwikkeling en het onderhoud van de standaarden is voor ten minste drie jaar gegarandeerd.

Experts adviseren dat het NCSC een actieve rol op zich neemt binnen de Technical Committee (TC) van OASIS, bij voorkeur ook met vertegenwoordiging in het bestuur. Dit zodat de Nederlandse belangen voldoende vertegenwoordigd worden bij ontwikkelingen rondom deze standaard

5.2.4.2 Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?

Ja, OASIS houdt rekening met verschillende belangen door een transparant en inclusief proces te hanteren waarbij diverse belanghebbenden kunnen deelnemen en input kunnen geven.

5.2.4.3 Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?

Ja, belanghebbenden kunnen formeel bezwaar aantekenen tegen de gevolgde procedure.

5.2.4.4 (UB) Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?

Ja, OASIS organiseert regelmatig overleggen met belanghebbenden over de doorontwikkeling en het beheer van de standaard.

5.2.4.5 (NL_int) Wat doet de Nederlandse intermediair om deze overleggen in Nederland voldoende onder de aandacht te brengen?

Het NCSC is voornemens om vanuit haar regierol de overleggen over de doorontwikkeling en het beheer van de standaard door OASIS onder de aandacht in Nederland te brengen. Het NCSC benut daarbij zijn zichtbare positie in het Nederlandse cybersecurityveld en maakt gebruik van bestaande kanalen en samenwerkingsverbanden. Voorbeelden van te gebruiken kanalen zijn de NCSC-website, Mattermost-kanalen, het NCSC-Community forum (voorheen DTC community), zoals media (zoals LinkedIn), mailing en bijeenkomsten in persoon, zoals sectorale ISACs. Geschikte samenwerkingsverbanden om aandacht te genereren zijn onder meer het CWN en Cyclotron.

5.2.4.6 Organiseert de standaardisatieorganisatie een openbare consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?

Ja, voorafgaand aan de vaststelling van een nieuwe versie van de standaard organiseert OASIS een publieke consultatie.

5.2.4.7 (NL_int) Wat doet de Nederlandse intermediair om deze publieke consultatie actief onder de aandacht te brengen bij de Nederlandse overheid?

Het NCSC is voornemens om vanuit haar regierol de publieke consultatie die door OASIS wordt georganiseerd actief onder de aandacht bij de Nederlandse overheid. Het NCSC maakt daarbij gebruik van zijn zeer zichtbare positie binnen de cybersecurityactiviteiten en -organisatie van de Nederlandse overheid, en zet bestaande kanalen en samenwerkingsverbanden in. Voorbeelden van te gebruiken kanalen zijn de NCSC-website, Mattermost-kanalen, bijeenkomsten in persoon (zoals in gremia zoals het CIO Rijk-overleg) en persoonlijk relatiemanagement, waaronder ook de ISACs.

5.2.5 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

5.2.5.1 Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?

Ja, OASIS is een internationaal non-profit consortium dat zich richt op de ontwikkeling en adoptie van open standaarden voor informatie-uitwisseling. OASIS ontwikkelt standaarden die bijdragen aan interoperabiliteit en samenwerking tussen verschillende systemen en organisaties.

5.2.5.2 Is de financiering van de ontwikkeling en het onderhoud van de standaard voor ten minste drie jaar gegarandeerd?

Ja, OASIS bestaat al sinds 1993 en wordt gefinancierd door een combinatie van lidmaatschapsbijdragen, sponsoring en het organiseren van evenementen. Organisaties kunnen lid worden van OASIS en betalen jaarlijkse lidmaatschapskosten, die variëren afhankelijk van het type lidmaatschap (bijvoorbeeld voor bedrijven, non-profit organisaties of overheidsinstellingen). Daarnaast kunnen bedrijven en organisaties ook specifieke projecten of werkgroepen sponsoren, wat bijdraagt aan de financiering van de activiteiten van OASIS.

5.2.6 Is het (versie)beheer van de standaard goed geregeld?

5.2.6.1 (UB) Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot (versie)beheer van de standaard?

Ja, de standaardisatieorganisatie heeft een gepubliceerd beleid met betrekking tot versiebeheer van de standaarden. Dit beleid is beschreven in een beheerplan en beschikbaar via de website van OASIS. De beheerdocumentatie is goed vindbaar en verkrijgbaar via dezelfde bron.

5.2.6.2 (UB) Is de beheerdocumentatie goed vindbaar en verkrijgbaar?

Ja, de beheerdocumentatie is goed vindbaar en verkrijgbaar via de website van OASIS.

5.2.6.3 (UB) Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?

Ja, hoewel uit de evaluatie cluster 'Veilig Internet' blijkt dat er verbeterpunten zijn op het vlak van de borging van het belang van de Nederlandse overheid bij de ontwikkeling en het beheer van de standaard.

Experts adviseren dat het NCSC een actieve rol op zich neemt binnen de Technical Committee (TC) van OASIS, bij voorkeur ook met vertegenwoordiging in het bestuur. Dit zodat de Nederlandse belangen voldoende vertegenwoordigd worden bij ontwikkelingen rondom deze standaard.

5.2.6.4 (NL_int) Wat doet de Nederlandse intermediair om het Nederlands belang voldoende te borgen? Op welke wijze wordt gecontroleerd of Nederlandse inbreng ook daadwerkelijk wordt opgepakt?

Het NCSC is voornemens om vanuit haar regierol de inbreng van Nederlandse organisaties tijdens openbare consultaties, en bij deelname aan publiek aangekondigde overleggen van OASIS te monitoren. Daarnaast haalt het NCSC periodiek via een enquête onder het initiatief SecureNed, Cyclotron en/of de NCSC Community forum of portaal het beeld op bij Nederlandse belanghebbenden om te beoordelen of het Nederlandse belang voldoende is meegenomen.

5.2.6.5 (UB) Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard?

Onbekend, de vertegenwoordiging van belanghebbenden bij het beheer van de standaard is niet onderzocht. Wel blijkt uit de press release dat een veelheid en diversiteit aan grote bedrijven positief staat tegenover de standaard.

5.2.6.6 (NL_int) Wat doet de Nederlandse intermediair om het Nederlandse belang bij het beheer van de standaard voldoende te borgen?

Het NCSC is voornemens om vanuit haar intermediaire rol te onderzoeken op welke wijze aansluiting kan worden gezocht bij OASIS als beheerder van de standaard en om het Nederlandse belang onder de aandacht van de beheerder te brengen.

Experts hebben hierover een aanvullend advies gegeven, zie 5.2.6.3.

5.2.6.7 (UB) Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard?

Ja, het standaardisatieproces en de organisatie achter deze standaarden zijn dermate volwassen en hebben een bewezen trackrecord, dat aanvullende toetsing mogelijk achterwege gelaten kan worden. Hierbij is het wel noodzakelijk dat een nationale regierol voor de standaarden wordt ingevuld. De experts constateren dat NCSC de regierol formeel kan invullen, maar dit nog niet volledig doet. Er is behoefte dat NCSC deze rol actiever oppakt, zie 5.2.1. OASIS Open fungeert als aanspreekpunt waar meer informatie over de standaarden beschikbaar is. Ook kan de OASIS community hiervoor worden benaderd.

5.2.6.8 (NL_int) Wat is de rol van de internationale standaardisatieorganisatie, wat is de rol van de Nederlandse intermediair en hoe versterken deze elkaar?

De internationale standaardisatieorganisatie OASIS is de beheerder en eigenaar van de standaard. Het NCSC heeft de intentie om vanuit haar regierol als intermediair tijdig relevante ontwikkelingen richting OASIS en richting Nederlandse belanghebbenden te signaleren. 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.

5.2.7 Is er adoptieondersteuning voor de standaard?

5.2.7.1 (UB) Is er een toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaard is te vinden en op te vragen is?

Ja, er is een toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaarden is te vinden en op te vragen. Naast de internationale beheerfunctie van OASIS 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 versie 2.1. De gespreksnotitie benadrukt het belang van een actieve regierol van het NCSC bij het beheer en de toepassing van deze standaarden. De experts onderschrijven deze oproep en hebben hier een aanvullend advies over geformuleerd, zie 5.2.1.

Cybersecurity wordt in toenemende mate benaderd vanuit het perspectief van dreigingen en risico's, zoals benoemd in de Nederlandse Cybersecuritystrategie 2022-2028. Het ligt dan ook in de lijn der verwachting dat de overheid een sturende rol wil innemen op standaarden die betrekking hebben op dreigingsinformatie. Het NCSC kan deze regierol vervullen en levert daarmee een bijdrage aan het succes van de implementatie van STIX en TAXII versie 2.1 in Nederland.

5.2.7.2 (NL_int) Is er een toegankelijk nationaal aanspreekpunt of organisatie?

Ja, het NCSC is voornemens om vanuit haar regierol als nationaal aanspreekpunt te fungeren. Hiervoor wordt een duidelijke pagina op de website ingericht. Het NCSC is echter niet de beheerder van de standaard en kan verzoeken tot aanpassingen daarom alleen als belang doorgeven aan de beheerder, OASIS. Wel kan het NCSC generieke ondersteuning bieden bij het gebruik van de standaard door middel van kennisdocumenten.

5.2.7.3 (UB) Wordt er ondersteuning gegeven in de adoptie en de implementatie van de standaard?

Ja, zie het antwoord bij paragraaf 5.2.7.1.

5.2.7.4 (NL_int) Wordt er vanuit een Nederlandse organisatie ondersteuning gegeven in de adoptie en de implementatie van de standaard?

Ja, het NCSC is voornemens om een trekkende rol te vervullen in verschillende standaardisatieprocessen, waaronder STIX en TAXII versie 2.1. Een onderdeel van de standaardisatieactiviteiten van het NCSC is het ondersteunen van de adoptie door middel van (vertaalde) publicaties over standaarden, zowel zelf opgesteld als gedeeld van andere organisaties. Daarnaast neemt het NCSC een actieve rol in relevante overleggen voor belanghebbenden, zowel nationaal als binnen de EU, voor geselecteerde standaarden zoals STIX en TAXII versie 2.1.

5.3 Draagvlak

Met dit criterium wordt bepaald of de opname van de standaard op de 'Pas toe of leg uit'-lijst of lijst aanbevolen standaarden op voldoende breed draagvlak kan rekenen binnen de overheid. Een voorwaarde hierbij is ook dat er voldoende marktondersteuning voor de standaard bestaat en dat het marktaanbod evenwichtig is (dus geen leveranciersafhankelijkheid in de hand werkt).

5.3.1 Waardering van het criterium criteria 'draagvlak'

De experts komen tot de conclusie dat STIX en TAXII versie 2.1 voldoet aan het criterium 'draagvlak'. Deze conclusie wordt in de volgende paragrafen toegelicht.

5.3.2 Bestaat er voldoende marktondersteuning voor de standaard?

5.3.2.1 Bieden meerdere leveranciers ondersteuning voor de standaard?

Ja, meerdere leveranciers bieden ondersteuning en het zijn breed geaccepteerde standaarden voor het verkrijgen en verstrekken van dreigingsinformatie. STIX en TAXII versie 2.1 gelden binnen de markt voor cyberindringingsdetectie en dreigingsinformatie als de toonaangevende standaarden. Verschillende commerciële partijen passen deze standaarden toe in hun producten. Een overzicht van commerciële en opensource-implementaties is beschikbaar via de OASIS-wiki. Sommige implementaties bevatten leverancier-specifieke aanpassingen, zoals extra functionaliteit of eigen datavelden. Omdat deze oplossingen mogelijk niet volledig conform de standaarden zijn of niet formeel zijn geverifieerd, wordt terughoudend omgegaan met formele erkenning. Tegelijkertijd vinden gesprekken plaats over de mogelijkheden en beperkingen van dergelijke toepassingen. Systemen voor interoperabiliteitschecks kunnen hierin een rol spelen.

5.3.2.2 Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?

Nee, een gebruiker kan de conformiteit van de implementatie van de standaard niet automatisch laten toetsen. Wel is er een tool beschikbaar die controleert of een STIX entiteit juist is. Daarnaast biedt het interoperabiliteitsprogramma de gebruiker de mogelijkheid om te toetsen of aan verschillende persona's wordt voldaan.

5.3.2.3 Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn om de standaard te implementeren of te gebruiken?

Ja, STIX versie 2.1 zorgt voor een gemeenschappelijk dataformaat en TAXII versie 2.1 verzorgt het transport. Er is ruimte voor lokale aanpassingen met bijvoorbeeld eigen velden, 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. Voor bepaalde standaarden kan een Nederlands profiel relevant zijn. De experts zijn van mening dat dit voor STIX en TAXII versie 2.1 in de Nederlandse context niet nodig is. Wat betreft de

soorten en typen data: organisaties gebruiken hun eigen typen data, zoals verschillende betrouwbaarheidsniveaus binnen het STIX-model. Dit is echter al in het model opgenomen en hoeft niet apart toegevoegd te worden. Het is onderdeel van de standaard en sluit aan op het schema van het STIX-model.

TAXII versie 2.1 zorgt slechts voor het transport en daarom zijn profielen daar niet relevant.

5.3.2.4 Zijn er profielen of voorbeeldimplementaties van de standaard aanwezig en zijn deze vrij te gebruiken?

Ja, er zijn voorbeeldimplementaties van de standaard aanwezig en deze zijn vrij te gebruiken:

- Een implementatie voor het serializen en de-serializing van STIX versie 2.1 entiteiten;
- Een implementatie van een TAXII versie 2.1 server;
- Een implementatie van een TAXII versie 2.1 client.

Daarnaast zijn er interoperabiliteit documenten beschikbaar die aangeven hoe de standaard in bepaalde scenario's moet worden toegepast.

5.3.3 Kan de standaard rekenen op voldoende draagvlak?

5.3.3.1 Staan de belangrijkste stakeholders vanuit de overheid voor deze standaard achter de adoptie van de standaard?

Ja, de aanwezige experts staan achter de adoptie van de standaarden en zij zijn een goede vertegenwoordiging van de overheid. Zie ook de Evaluatie cluster 'Veilig Internet' en pagina 17-20 van de inventarisatie gebruiksgegevens 2024. De adoptie van deze standaard ondersteunt tevens de zorgplicht en het stelsel van de Cbw.

5.3.3.2 Staan de overheidsorganisaties die worden geraakt door een verplichting van de standaard achter het verplichte gebruik van de standaard?

Ja, overheidsorganisaties die daadwerkelijk worden geraakt door een mogelijke verplichting van de standaarden lijken het gebruik ervan te ondersteunen. Hoewel er geen empirisch onderzoek naar is gedaan, heeft het NCSC 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. Veel organisaties passen de nieuwe versie van de standaarden al toe. Ook de aanwezige sectorale CSIRTs spreken hun steun uit voor de standaarden. 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.

5.3.3.3 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?

Ja, veel organisaties passen de nieuwe versie van de standaarden al toe. Binnen het organisatorische werkingsgebied wordt de aangemelde versie van de standaarden door

meerdere Nederlandse overheidsorganisaties gebruikt. Aangezien het NCSC de standaarden toepast voor hun doelgroep, zullen andere Rijksoverheidsorganisaties deze standaarden ook hanteren wanneer zij dreigingsinlichtingen data willen verkrijgen met en verstrekken aan het NCSC. Uit de Evaluatie cluster 'Veilig Internet' blijkt dat gebruik bij gemeenten en waterschappen achterblijft. Experts geven aan dat dit nog steeds het geval is, maar dat hier wel verbetering zichtbaar is.

Een expert namens de provincies meldt dat de provincie bezig is met een traject richting de inrichting van een SOC. Een expert namens de gemeenten geeft aan dat de adoptie goed verloopt, maar dat het daadwerkelijke gebruik nog achterblijft.

Namens de waterschappen was geen vertegenwoordiger aanwezig bij de expertbijeenkomst. CERT-WM zal worden gevraagd een reactie aan te leveren wanneer het expertadvies wordt aangeboden ter openbare consultatie op internetconsultatie.nl.

5.3.3.4 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?

Ja, een vorige versie van de standaarden wordt ook binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt, al zijn hier lastig concrete cijfers aan te koppelen. Zie opnieuw pagina 17-20 van de inventarisatie gebruiksgegevens 2024.

5.3.3.5 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?

Nee, de aangemelde versie 2.1 is niet backwards compatible met eerdere versies van de standaarden.

5.3.3.6 Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?

Ja, er zijn voldoende positieve signalen over het huidige en toekomstige gebruik van de standaarden door (semi-)overheidsorganisaties, het bedrijfsleven en burgers. Zie hierover het evaluatierapport. Binnen de sector informatiebeveiliging is al afgestapt van STIX versie 1.2.1 en TAXII 1.1.1 en is gebruik van versie 2.1 inmiddels de facto de standaard.

5.4 Opname op de lijst bevordert adoptie

De experts komen tot de conclusie 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. Het verhoogt de bekendheid en daarmee de adoptie van de standaard door organisaties. De nieuwe versie 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 haar 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 de standaarden 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 aanwezige sectorale CSIRTs zien de meerwaarde van de standaarden en opname op de lijst.

6 Adviezen bij opname van de standaard

De experts geven het Forum Standaardisatie en 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 invulling aan criteria voor het verkrijgen van het predicaat 'Uitstekend beheer' voor Nederlandse intermediair (Erkend Nederlands Intermediair) en opvolging aan gestelde adoptieadviezen toen STIX en TAXII eind 2017 op de 'Pas toe of leg uit' werd geplaatst. 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).

6.1 Adviezen bij opname versie 2.1 STIX en TAXII

1. Experts adviseren 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. Experts adviseren 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. Experts adviseren 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. Experts adviseren het Forum Standaardisatie om een expertbijeenkomst te organiseren 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. NCSC neemt zelf het initiatief door bij het Forum Standaardisatie te melden dat het gereed is voor deze toetsing.

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

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

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

(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.

6.3 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).