Forum Standaardisatie

Expertadvies voor opname STIX 1.2.1 en TAXII 1.1.1 op de 'pas toe of leg uit' lijst

Concept ter openbare consultatie

Datum 31 juli 2017

Colofon

Projectnaam	Expertadvies STIX 1.2.1 en TAXII 1.1.1
Versienummer	1.1
Locatie	Den Haag
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag info@forumstandaardisatie.nl
Auteur	Paul Dam
Onafhankelijk voorzitter	Wilbert Enserink

Inhoud

Samenvatting en Forumadvies

Advies aan het Forum
De expertgroep adviseert het Forum Standaardisatie en het Nationaal Beraad Digitale Overheid om STIX 1.2.1 en TAXII 1.1.1 op te nemen op de 'pas toe of leg uit'-lijst.

Als functioneel toepassingsgebied wordt geadviseerd:

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

Als organisatorisch werkingsgebied wordt geadviseerd:

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

Waarom is opname belangrijk?
Opname van deze standaarden is van belang omdat deze standaarden het mogelijk maken om gestructureerde dreigingsinformatie over digitale dreigingen tegen informatiesystemen breed en eenvoudig te delen tussen overheidsorganisaties. Dit verhoogt de digitale weerbaarheid van de overheid en instellingen in de (semi-) publieke sector. Opname op de lijst stimuleert de verdere adoptie van deze standaarden voor geautomatiseerd delen van dreigingsinformatie (binnen de overheid).

Waar gaat het inhoudelijk over?
STIX is een gestructureerde taal om dreigingsinformatie te beschrijven zodat het op een consistente manier kan worden gedeeld, opgeslagen en geanalyseerd. Via deze taal kunnen objecten zoals Incident, Indicator, Campaign en Course of Action worden beschreven. Gestructureerde dreigingsinformatie in het STIX-formaat kan geautomatiseerd verwerkt worden door onder andere beveiligingsapparatuur en –tooling. STIX 1.x maakt gebruik van XML als bestandsformaat.

TAXII is een transportmechanisme dat het geautomatiseerd uitwisselen van dreigingsinformatie standaardiseert. Het maakt gebruik van push/pull mechanismen op basis van abonnementen of kanalen en maakt voor het transport gebruik van HTTPS. TAXII kan worden gebruikt voor het uitwisselen van dreigingsinformatiedocumenten in STIX-formaat.

Hoe is het proces verlopen?
Het Bureau Forum Standaardisatie heeft een intakegesprek gevoerd met de indiener van de standaarden STIX 1.2.1 en TAXII 1.1.1. Tijdens de intake zijn de standaarden getoetst op uitsluitingscriteria en is een eerste inschatting gemaakt van de kansrijkheid van de procedure. Naar aanleiding daarvan heeft het Forum Standaardisatie besloten de standaarden in procedure te nemen.

Vervolgens is een expertgroep samengesteld die op 4 juli 2017 bijeenkwam. De uitkomsten van de expertgroep, waaronder de vaststelling van het toepassings- en werkingsgebied, zijn door de voorzitter en begeleider verwerkt in dit adviesrapport, dat ter publieke

consultatie wordt aangeboden voorafgaand aan besluitvorming door het Forum Standaardisatie.

Hoe scoort de standaard op de toetsingscriteria?

Toegevoegde waarde
Er is nog geen andere standaard die gaat over het uitwisselen van gestructureerde dreigingsinformatie. STIX 1.2.1 en TAXII 1.1.1 zijn de meest breed ondersteunde standaarden op dit gebied. Alleen OpenIOC is een standaard die voor een deel van het voorgestelde functionele toepassingsgebied een alternatief biedt. Om te voorkomen dat voor iedere koppeling uitgezocht moet worden hoe gestructureerde dreigingsinformatie kan worden uitgewisseld is het opnemen van deze standaard noodzakelijk. Door STIX 1.2.1 en TAXII 1.1.1 op te nemen op de lijst kan voorkomen worden dat vendor lock-in ontstaat door eigen formaten van leveranciers.

Met STIX 1.2.1 en TAXII 1.1.1 alleen is de interoperabiliteit nog niet gegarandeerd. STIX Profielen definiëren een subset van de STIX-objecten en attributen. Ze kunnen worden gebruikt om aan te geven dat slechts een subset van STIX wordt ondersteund of geproduceerd. Er is geen "de facto" STIX-profiel aan te wijzen. In beginsel staat een gebruiker de volledige STIX-standaard ter beschikking, maar als er een beperkt aandachtsgebied is of met een incomplete STIX-implementatie wordt gewerkt, kan het zinvol zijn dit te beschrijven in een STIX profiel. Het is denkbaar dat als STIX binnen de overheid meer gebruikt gaat worden er STIX-profielen worden opgesteld en op elkaar worden afgestemd. Het is nu echter te vroeg om al een STIX overheidsprofiel op te stellen en voor te schrijven. De indiener adviseert dan ook om STIX 1.2.1 zonder beperkend STIX-profiel als standaard op te nemen.

De beveiligingsrisico's aan de uitwisseling van dreigingsinformatie worden met deze standaard gemitigeerd door (tweezijdige) authenticatie en encryptie, door het gebruik van TLS. Privacyrisico's kunnen worden beheerst door een privacybeleid bijpassend bij de uitwisseling van dreigingsinformatie.

Open standaardisatieproces
STIX en TAXII worden beheerd door OASIS, een internationale onafhankelijke non-profit standaardisatieorganisatie, die de specificaties zonder belemmeringen beschikbaar stelt op haar website. Het intellectueel eigendomsrecht op de standaard stelt OASIS onherroepelijk royalty-free voor eenieder beschikbaar onder de OASIS Intellectual Property Rights Policy.

Het besluitvormingsproces van de standaard is toegankelijk voor iedereen die lid is van de OASIS Cyber Threat Intelligence Technical Committee. Iedereen kan lid worden. Het beheerproces voldoet ook overigens aan de eisen die het Forum stelt, zoals de mogelijkheid tot bezwaar, gepubliceerd beleid met betrekking tot versiebeheer en toegankelijke beheerdocumentatie.

De indiener raadt af het predicaat 'Uitstekend beheerproces' toe te kennen, doordat grote wijzigingen die doorgevoerd kunnen worden het wenselijk is om aanvullende toetsing plaats te laten vinden.

Draagvlak
De standaarden STIX 1.2.1 en TAXII 1.1.1 zijn inmiddels in gebruik bij het NCSC, de Belastingdienst, Rijkswaterstaat en SSC-ICT. De standaarden STIX en TAXII worden ondersteund door onder andere de leveranciers Splunk, HP ArcSight, IBM QRadar, Alienvault, EclecticIQ, ThreatConnect, Anomali en ThreatQuotient. Ook is er open source tooling beschikbaar om een implementatie te valideren.

De standaard is relevant voor alle overheidsorganisaties (Rijk, provincies, gemeenten) en instellingen in de (semi-) publieke sector die in het kader van hun informatiebeveiliging gestructureerde dreigingsinformatie verzamelen en uitwisselen. Denk hierbij in het bijzonder aan Security Operations Centers. De CTO-Raad van de Rijksoverheid, het RijksISAC en de nformatiebeveiligingsdienst voor gemeenten (IBD) ondersteunen expliciet de aanmelding van deze standaard bij het Forum Standaardisatie.

Opname bevordert de adoptie
De opname op de lijst moet een geschikt middel zijn om de adoptie van de standaard te bevorderen. Het geautomatiseerd delen van dreigingsinformatie (binnen de overheid) staat nog aan het begin, evenals de adoptie van standaarden voor deze gegevensuitwisseling. Het plaatsen van de STIX- en TAXII-standaarden op de lijst open standaarden stimuleert het gebruik van deze standaarden en zal zo zorgen voor betere interoperabiliteit. Er ontstaat momentum voor de standaarden en opname als verplichte standaard (pas-toe-of-leg-uit) op de lijst open standaarden kan dit momentum vergroten.

Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?
De expertgroep doet het Nationaal Beraad de aanbeveling om bij de opname op de lijst voor 'pas toe of leg uit' de volgende oproepen ten aanzien van de adoptie van STIX en TAXII te doen:

- Het Forum roept het NCSC op om samen met betrokkenen een leidraad op te stellen, al dan niet als onderdeel van een bestaand kennisproduct[1], 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.
- Het Forum 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.
- Het Forum 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.

[1] *Het NCSC en de AIVD hebben reeds een whitepaper over dit vraagstuk uitgebracht (zie https://www.ncsc.nl/actueel/whitepapers/handreiking-voor-implementatie-van-detectie-oplossingen.html). Daarnaast heeft het NCSC een factsheet over Indicators of Compromise uitgegeven (zie https://www.ncsc.nl/actueel/factsheets/factsheet-indicators-of-compromise.html).*

- Het Forum roept overheden die STIX en TAXII toepassen op om informatie over de meerwaarde van het gebruik voor hen en *best practices* te delen.
- Het Forum roept KING op om in de GGI (gemeentelijke gemeenschappelijke infrastructuur) STIX en TAXII toe te passen in het SOC (security operations center).

De expertgroep adviseert het Forum Standaardisatie de adoptie en deze oproepen na 2 jaar te evalueren.

1 Doelstelling expertadvies

1.1 Achtergrond

De Nederlandse overheid streeft naar betrouwbare gegevensuitwisseling door het gebruik van open standaarden en het voorkomen van vendor lock-in. Het actieplan "Open Overheid", de Digitale Agenda 2017 en de kabinetsreactie op het Rapport Elias benadrukken dit beleid. Om dit doel te bereiken, onderstrepen het instellingsbesluit van het Forum Standaardisatie, de Generieke Digitale Infrastructuur en de verschillende architectuurkaders het gebruik van open standaarden bij het ontwerpen of inkopen van informatiesystemen.

Een van de maatregelen om de adoptie van open standaarden te bevorderen is de publicatie en het beheer van een lijst met open standaarden waarvoor een 'pas toe of leg uit' verplichting geldt of waarvan het gebruik 'aanbevolen' is. Het Nationaal Beraad Digitale Overheid (hierna Nationaal Beraad) besluit welke standaarden op deze lijst worden opgenomen. Het Nationaal Beraad baseert zich hierbij op expertadviezen, openbare consultaties en adviezen van het Forum Standaardisatie.

1.2 Doelstelling expertadvies

Dit document is een expertadvies voor STIX 1.2.1 en TAXII 1.1.1 gericht aan het Nationaal Beraad en Forum Standaardisatie. STIX 1.2.1 en TAXII 1.1.1 zijn aangemeld voor opname op de lijst met open standaarden door Arjan de Jong van het NCSC (Ministerie van Veiligheid en Justitie).

Doel van dit document is om het Nationaal Beraad te adviseren of STIX 1.2.1 en TAXII 1.1.1 in aanmerking komen voor opname op de lijst met open standaarden als 'pas toe of leg uit'-standaard, al dan niet onder voorwaarden.

1.3 Doorlopen proces

Voor het opstellen van dit proces is de volgende procedure doorlopen:

1. De procesbegeleider heeft op 12 mei 2017 een intakegesprek gevoerd met de indiener. Tijdens de intake is de standaard getoetst op criteria voor inbehandelname en is een eerste inschatting gemaakt van de kansrijkheid van de procedure.
2. Op basis van de intake heeft het Forum Sandaardisatie op 14 juni 2017 besloten de aanmelding in procedure te nemen. Hierop volgend is een expertgroep samengesteld en een voorzitter aangesteld.
3. De leden van de expertgroep hebben een voorbereidingsdossier gekregen dat is samengesteld met informatie uit de aanmelding en het intakeonderzoek. Voorafgaand aan de expertbijeenkomst heeft de expertgroep dit voorbereidingsdossier doorgenomen en aandachtspunten geïdentificeerd.
4. De expertgroep is op 4 juli 2017 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgesteld.

Dit expertadvies geeft de uitkomst van de bespreking door de expertgroep weer. De procesbegeleider heeft een concept van dit expertadvies aan de leden van de expertgroep gestuurd met verzoek om commentaar. Na

verwerking van reacties uit de expertgroep is het rapport nogmaals toegestuurd aan de experts, afgerond en ingediend bij het Bureau Forum Standaardisatie (het secretariaat van het Forum Standaardisatie) ten behoeve van de publieke consultatieronde.

1.4 Vervolg

Het Bureau Forum Stadaardisatie stelt dit expertadvies openbaar ten behoeve van een publieke consultatie die plaatsvindt van 1 augustus 2017 tot 13 september 2017. Eenieder kan gedurende de consultatieperiode een reactie geven op dit expertadvies. Na afsluiting van de openbare consultatie koppelt het Bureau Forum Standaardisatie de reacties terug aan de expertgroep.

Het Forum Standaardisatie stelt met het expertadvies en de relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad op. Het Nationaal Beraad besluit met dit advies om de standaard wel of niet op de lijst open standaarden te plaatsen.

1.5 Samenstelling expertgroep

Het Forum Standaardisatie streeft naar een representatieve expertgroep met een evenwichtige vertegenwoordiging van (toekomstige) gebruikers (zowel publiek als privaat), leveranciers, wetenschappers en andere belanghebbenden. De expertgroep heeft een onafhankelijk voorzitter die de expertgroep leidt en de verantwoordelijkheid neemt voor het expertadvies.

Als onafhankelijk voorzitter is opgetreden Wilbert Enserink, managing consultant bij Verdonck, Klooster & Associates. Paul Dam, management consultant bij Verdonck, Klooster & Associates, heeft de procedure in opdracht van het Bureau Forum Standaardisatie begeleid.

Aan de expertbijeenkomst hebben deelgenomen:

Organisatie	Persoon
KPN	Daan Planqué
Shell	Dohan Jansen
DUO	Erik Veenstra
IBD	John van Huijgevoort
SURFnet	Melvin Koelewijn
EclecticIQ	Aukjan van Belkum
FOX-IT	Gaetan van Diemen
SMT/ SPLUNK	Bernardo Dijkland Arnold Holzel
NCSC	Arjan de Jong Richard van den Berg

Han Zuidweg van het Bureau Forum Standaardisatie was als toehoorder bij de expertbijeenkomst aanwezig.

1.6 Toelichting STIX en TAXII

Relatie met andere verplichte standaarden
De standaard TAXII bouwt voort op https (TLS), IPv4/IPv6. Daarnaast is er samenhang met ISO 27001/27002, in de zin dat STIX en TAXII voor een aantal overheidsorganisaties invulling kan geven aan maatregelen die

zij op basis van ISO 27001/27002 voor zichzelf gedefinieerd hebben. Dit heeft geen gevolgen voor de toetsing van STIX en TAXII.

Relatie met andere aanbevolen standaarden
De standaard TAXII bouwt voort op XML en URI. Dit heeft geen gevolgen voor de toetsing van STIX en TAXII.

Relatie met overige standaarden
De standaarden STIX en TAXII bouwen voort op de andere standaarden, zoals (zover hierboven nog niet genoemd):
- Common Attack Pattern Enumeration and Classification (CAPEC)
- Common Event Expression (CEE)
- Customer Information Quality (CIQ)
- Common Platform Enumeration (CPE)
- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerabilites Reporting Framework (CVRF)
- Common Weakness Enumeration (CWE)
- Date and time format – ISO 8601
- Malware Attribute Enumeration and Characterization (MAEC)
- Open Indicators of Compromise (OpenIOC)
- Open Vulnerability and Assessment Language (OVAL)
- Cyber Observable Expression (CybOX)

In de procedure is kort onderzoek verricht naar de mate waarin deze standaarden voldoen aan de criteria van het Forum Standaardisatie voor opneming op de lijst open standaarden.

1.7 Leeswijzer

Hoofdstuk 2 beschrijft het functioneel toepassingsgebied (situaties waarin de standaard functioneel gebruikt moet worden) en het organisatorisch werkingsgebied (organisaties die de standaard moeten toepassen).

Hoofdstuk 3 beschrijft de resultaten van de toetsing van de standaard aan de hand van de criteria voor opname op de lijst open standaarden.

2 Toepassings– en werkingsgebied

De *instructie rijksdienst inzake de aanschaf van ICT producten en ICT diensten* verplicht overheidsorganisaties om relevante standaarden op de 'pas toe of leg uit'-lijst te vragen en toe te passen bij aanbestedingstrajecten.

Afhankelijk van de aan te schaffen functionaliteit moet een overheidsorganisatie bepalen welke standaarden op de 'pas toe of leg uit'-lijst relevant zijn. Hiervoor is voor iedere standaard een *functioneel toepassingsgebied* (in welke situaties is de standaard functioneel van toepassing) en een *organisatorisch toepassingsgebied* (welke oranisaties moeten de standaard gebruiken) beschreven.

Secties 2.1 en 2.2 geven het advies van de expertgroep voor het functioneel en organisatorisch toepasingsgebied van STIX en TAXII.

2.1 Functioneel toepassingsgebied

De expertgroep adviseert als functioneel toepassingsgebied voor STIX 1.2.1 en TAXII 1.1.1:

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

Toelichting
De term *gestructureerde uitwisseling* is gebruikt om aan te duiden dat uitwisseling plaatsvindt in de vorm van berichten met een specifieke gestandaardiseerde indeling in betekenisvolle gegevenselementen. Het gaat dan in de praktijk altijd over uitwisseling van gegevens tussen geautomatiseerde informatiesystemen.

Het gebruik van de term *digitale dreigingen* beperkt het functioneel toepassingsgebied door andersoortige dreigingen, zoals fysieke dreigingen, uit te sluiten.

Daarnaast moet het gaan om de dreiging tegen *informatiesystemen*, of althans de goede werking, integriteit en beschikbaarheid van informatiesystemen.

2.2 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied van de standaard overeen te laten komen met het werkingsgebied waarop de 'pas toe of leg uit' verplichting van toepassing is, te weten:

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

3 Toetsing van standaard aan criteria

Het Forum Standaardisatie hanteert vier hoofdcriteria om te bepalen of een standaard in aanmerking komt voor opname op de lijst:
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 nodig om de adoptie te bevorderen?[2]

Ieder van deze hoofdcriteria heeft deelcriteria die beschreven staan in het document *"Toetsingsprocedure en criteria voor lijst met open standaarden voor indieners en experts",* te vinden op de website van het Forum Standaardisatie https://www.forumstandaardisatie.nl/content/toetsen-van-standaarden.

Dit hoofdstuk beschrijft per criterium het resultaat van de toetsing. Voor de volledigheid is tevens de beschrijving van elk criterium opgenomen.

3.1 Toegevoegde waarde

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen.

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

3.1.1.1 Is het functioneel toepassingsgebied goed gedefinieerd?
Ja, zie paragraaf 2.1.

3.1.1.2 Is het organisatorisch werkingsgebied goed gedefinieerd?
Ja, zie paragraaf 2.2.

3.1.1.3 Is de standaard generiek toepasbaar (en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke organisaties)? (toelichtende vraag)
Ja, de standaard is breed toepasbaar door overheden die gestructureerde dreigingsinformatie willen uitwisselen.

3.1.2 Verhoudt de standaard zich goed tot andere standaarden?

3.1.2.1 Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?
De standaard TAXII bouwt voort op https (TLS), IPv4/IPv6. Daarnaast is er samenhang met ISO 27001/27002, in de zin dat STIX en TAXII voor een aantal overheidsorganisaties invulling kan geven aan maatregelen die zij op basis van ISO 27001/27002 voor zichzelf gedefinieerd hebben. De standaarden STIX en TAXII kunnen daardoor naast deze standaarden op de 'pas toe of leg uit'-lijst opgenomen worden.

2 Dit criterium is voornamelijk van toepassing op standaarden op de 'pas toe of leg uit' lijst, niet voor aanbevolen standaarden.

De standaard TAXII bouwt voort op XML en URI. De standaarden STIX en TAXII hebben daardoor meerwaarde boven deze standaarden.

3.1.2.2 Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied? (Dit kan ook om een nieuwe versie van dezelfde standaard gaan.)

Ja, er is nog geen andere opgenomen standaard die gaat over de gestructureerde uitwisseling van informatie over digitale dreigingen tegen informatiesystemen.

Strikt genomen overlapt het functioneel toepassingsgebied van TAXII met dat van Digikoppeling. Technisch verschillen Digikoppeling en TAXII echter in functionaliteit. TAXII een publish-subscribe protocol; Digikoppeling ondersteunt deze vorm van berichtenverkeer slechts indirect.

In bestaande implementaties van STIX is het alleen mogelijk om STIX-documenten over TAXII uit te wisselen of over een aanbieder-specifiek koppelvlak (API). Het uitwisselen van STIX-documenten over Digikoppeling ligt daardoor niet voor de hand.

3.1.2.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? (toelichtende vraag)

Ja, geen andere standaard is zo compleet en zo breed ondersteund als STIX en TAXII.

OpenIOC en IODEF (RFC5070, 2007/RFC7970 2016) zijn alternatieve standaarden voor slechts een deel van de functionaliteit. Zelfs met de Extension for Structured Cybersecurity Information (RFC7203, 2014) is IODEF niet zo uitgebreid als STIX. Technisch gesproken is het mogelijk om IODEF in STIX te gebruiken als beschrijving voor incidentinformatie (beiden zijn XML) maar in de praktijk zijn hier geen implementaties van bekend. STIX wordt door diverse security producten ondersteund terwijl IODEF voornamelijk in de IDS/IPS producten populair is.

De standaarden STIX en TAXII bouwen voort op andere standaarden, zoals (zover hierboven nog niet genoemd):

- Common Attack Pattern Enumeration and Classification (CAPEC)
- Common Event Expression (CEE)
- Customer Information Quality (CIQ)
- Common Platform Enumeration (CPE)
- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerabilites Reporting Framework (CVRF)
- Common Weakness Enumeration (CWE)
- Date and time format – ISO 8601
- Malware Attribute Enumeration and Characterization (MAEC)
- Open Vulnerability and Assessment Language (OVAL)
- Cyber Observable Expression (CybOX)

Uit kort onderzoek naar de mate waarin deze standaarden voldoen aan de criteria van het Forum Standaardisatie blijkt dat al deze standaarden, in vergelijkbare mate als STIX en TAXII, voldoen aan de criteria van het Forum Standaardisatie.

3.1.2.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)
Ja, STIX en TAXII zijn internationale standaarden.

3.1.3 Wegen de kwantitatieve en kwalitatieve voordelen van adoptie van de standaard, voor de (semi-)overheid als geheel en voor de maatschappij, op tegen de nadelen?

3.1.3.1 Zijn de kosten van implementatie acceptabel en zijn deze kosten bekend en inzichtelijk?
Ja, de standaarden STIX en TAXII zijn zonder kosten beschikbaar. Veel bekende producten ondersteunen de standaarden al. Zonder gebruik van deze standaarden moeten steeds aparte afspraken worden gemaakt voor de uitwisseling van gestructureerde dreigingsinformatie. Het gebruik van STIX en TAXII is daardoor efficiënter. Specifieke kosten van implementatie van STIX en TAXII zijn niet bekend.

3.1.3.2 Is er een (kwalitatieve) businesscase van de standaard aanwezig?
Nee, er is nog geen businesscase geformuleerd.

3.1.3.3 Is de meerwaarde van de standaard goed inzichtelijk te maken? Wat betekent de standaard voor de (bedrijfs)processen van een organisatie of keten en wat los je met de standaard op?
Ja, door de toename aan digitale dreigingen is er een grote behoefte aan interoperabele en efficiënte uitwisseling en verwerking van dreigingsinformatie. STIX en TAXII standaardiseren de uitwisseling van dreigingsinformatie. Doordat de standaard open is en door meerdere leveranciers wordt toegepast neemt de leveranciersafhankelijkheid af.

Door het gebruik van STIX en TAXII wisselen het NCSC, de Belastingdienst, Rijkswaterstaat en SSC-ICT op een gestandaardiseerde manier dreigingsinformatie uit. Zonder de standaarden STIX en TAXII hadden specifieke afspraken gemaakt moeten worden voor iedere koppeling tussen deze organisaties.

3.1.3.4 Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?
Ja, de opname van STIX/TAXII als standaard zal juist bijdragen aan het afnemen van de beveiligingsrisico's. De beveiligingsrisico's aan de uitwisseling van dreigingsinformatie worden met deze standaard gemitigeerd door (tweezijdige) authenticatie en encryptie, door het gebruik van TLS.

3.1.3.5 Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?
Ja, de privacygevoelige informatie die met STIX en TAXII kan worden uitgewisseld betreft doorgaans informatie over aanvallers van digitale omgevingen. De daaraan verbonden privacyrisico's wegen over het algemeen op tegen het doel van het delen van deze informatie: het verhogen van de digitale weerbaarheid van de (semi-) overheidsorganisaties. Privacyrisico's kunnen worden beheerst door een privacybeleid bijpassend bij de uitwisseling van dreigingsinformatie.

Het is de verantwoordelijkheid van de gebruikers van STIX en TAXII om bij het uitwisselen van informatie de geldende privacyregelgeving te hanteren en een eigen afweging te maken van de privacyrisico's.

3.1.4 Conclusie criteria 'Toegevoegde waarde'

Er is nog geen andere standaard die het uitwisselen van gestructureerde dreigingsinformatie faciliteert. STIX en TAXII zijn de meest breed ondersteunde standaarden op dit gebied. Alleen OpenIOC is een standaard die voor een deel van het voorgestelde functionele toepassingsgebied een alternatief biedt. Om te voorkomen dat voor iedere koppeling uitgezocht moet worden hoe gestructureerde dreigingsinformatie kan worden uitgewisseld is het opnemen van deze standaard noodzakelijk. Door STIX en TAXII op te nemen op de lijst kan voorkomen worden dat vendor lock-in ontstaat door eigen formaten van leveranciers.

Met STIX en TAXII alleen zijn de voordelen van uitwisseling van gestructureerde dreigingsinformatie nog niet gerealiseerd. STIX Profielen definiëren een subset van de STIX-objecten en attributen. Ze kunnen worden gebruikt om aan te geven dat slechts een subset van STIX wordt ondersteund of geproduceerd. Er is geen "de facto" STIX-profiel aan te wijzen. In beginsel staat een gebruiker de volledige STIX-standaard ter beschikking, maar als er een beperkt aandachtsgebied is of met een incomplete STIX-implementatie wordt gewerkt, kan het zinvol zijn dit te beschrijven in een STIX profiel. Het is denkbaar dat als STIX binnen de overheid meer gebruikt gaat worden er STIX-profielen worden opgesteld en op elkaar worden afgestemd. Het is nu echter te vroeg om al een STIX overheidsprofiel op te stellen en voor te schrijven. De indiener adviseert dan ook om STIX 1.2.1 zonder beperkend STIX-profiel als standaard op te nemen, maar wel richtlijnen op te stellen voor het gebruik van de standaard (zie ook de adoptieadviezen ten aanzien van de op te stellen leidraad voor het gebruik van STIX en TAXII).

De beveiligingsrisico's aan de uitwisseling van dreigingsinformatie worden met deze standaard gemitigeerd door (tweezijdige) authenticatie en encryptie, door het gebruik van TLS. Privacyrisico's kunnen worden beheerst door een privacybeleid bijpassend bij de uitwisseling van dreigingsinformatie.

3.2 Open standaardisatieproces

De ontwikkeling en het beheer van de standaard zijn op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht.

3.2.1 Is de documentatie voor een ieder drempelvrij beschikbaar?

3.2.1.1 Is het specificatiedocument beschikbaar zonder dat er sprake is van belemmeringen (zoals hoge kosten of lidmaatschapseisen)?
Ja: https://docs.oasis-open.org/cti/stix/v1.2.1/ en http://docs.oasis-open.org/cti/taxii/v1.1.1/.

3.2.1.2 Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving van de besluitvormingsprocedure) beschikbaar zonder dat er sprake is van belemmeringen (zoals hoge kosten of lidmaatschapseisen)?
Ja, zie https://www.oasis-open.org/policies-guidelines/tc-process.

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

3.2.2.1 Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard (bijvoorbeeld patenten of licenties) onherroepelijk royalty-free voor eenieder beschikbaar?
Ja, STIX/TAXII wordt gepubliceerd onder de OASIS Intellectual Property Rights Policy, zie https://www.oasis-open.org/policies-guidelines/ipr.

3.2.2.2 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, dat is geregeld in secties 5.2 en 13.1 van de OASIS Intellectual Property Rights Policy, zie https://www.oasis-open.org/policies-guidelines/ipr.

3.2.3 Is de inspraak van eenieder in voldoende mate geborgd?

3.2.3.1 Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)?
Ja, iedereen kan lid worden van de OASIS Cyber Threat Intelligence Technical Committee die de STIX/TAXII standaard inhoudelijk beheert, zie https://www.oasis-open.org/policies-guidelines/tc-process.

3.2.3.2 Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?
Ja, zie https://www.oasis-open.org/policies-guidelines/tc-process.

3.2.3.3 Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?
Ja, zie https://www.oasis-open.org/policies-guidelines/tc-process#appeals.

3.2.3.4 Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?
Ja, zie https://www.oasis-open.org/policies-guidelines/tc-process#meetings. De huidige samenstelling van de OASIS CTI TC is te vinden op https://www.oasis-open.org/committees/cti.

3.2.3.5 Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?
Ja, zie https://www.oasis-open.org/policies-guidelines/tc-process#publicReview.

3.2.4 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

3.2.4.1 Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?
Ja, OASIS bestaat sinds 1993 en is onafhankelijk en duurzaam, zie https://nl.wikipedia.org/wiki/OASIS_%28organisatie%29.

3.2.4.2 Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?
Ja, de financiering van OASIS komt van haar leden en sponsoren, zie https://www.oasis-open.org/join/categories-dues en https://www.oasis-

open.org/member-roster. Met meer dan 5000 leden is de financiering langdurig gewaarborgd.

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

3.2.5.1 Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot (versie)beheer van de standaard? Bij voorkeur is dit beleid ook beschreven in een beheerplan (met o.a. aandacht voor migratie van gebruikers)
Ja, zie https://www.oasis-open.org/policies-guidelines/interoperability-guidelines en https://www.oasis-open.org/policies-guidelines/tc-process.

3.2.5.2 Is de beheerdocumentatie goed vindbaar en verkrijgbaar?
Ja, zie https://www.oasis-open.org/policies-guidelines/tc-process.

3.2.5.3 Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?
Ja. De Nederlandse overheid is zelf niet vertegenwoordigd in het Technical Comité dat de standaard beheert (zie https://www.oasis-open.org/committees/cti/). Echter, het brede internationale draagvlak voor de standaarden vermindert de noodzaak voor de Nederlandse overheid om direct bij de ontwikkeling en het beheer betrokken te zijn. De Nederlandse overheid zou lid kunnen worden van OASIS. Niet leden van de werkgroep kunnen bovendien ook commentaar insturen en zo een bijdrage aan de ontwikkeling van de standaard leveren, zie https://www.oasis-open.org/committees/comments/index.php?wg_abbrev=cti.

3.2.5.4 Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard?
Ja, de vertegenwoordiging in de werkgroep bestaat uit zowel gebruikers, publieke en private partijen, als aanbieders van de producten en diensten die gebruik maken van de standaarden. Zie https://www.oasis-open.org/committees/membership.php?wg_abbrev=cti.

3.2.5.5 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?
Nee, alhoewel iedere nieuwe versie van de specificatie met materiële wijzigingen een vaste set van stappen uit het TC proces met publieke consultaties doorloopt, is vanwege de grote wijzigingen die doorgevoerd kunnen worden het wenselijk om aanvullende toetsing plaats te laten vinden.

3.2.6 Is er adoptieondersteuning voor de standaard?

3.2.6.1 Is er een toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaard is te vinden en op te vragen is?
Alle specificaties en documentatie is vrij online beschikbaar op https://docs.oasis-open.org. Nadere informatie is ook te vinden bij leveranciers die de standaard ondersteunen.

3.2.6.2 *Wordt er ondersteuning gegeven in de adoptie en de implementatie van de standaard?*
Leveranciers en andere marktpartijen bieden ondersteuning bij de implementatie van de standaard.

3.2.7 Conclusie criteria 'Open standaardisatieproces'
STIX en TAXII worden beheerd door OASIS, een internationale onafhankelijke non-profit standaardisatieorganisatie, die de specificaties zonder belemmeringen beschikbaar stelt op haar website. Het intellectueel eigendomsrecht op de standaard stelt OASIS onherroepelijk royalty-free voor eenieder beschikbaar onder de OASIS Intellectual Property Rights Policy.

Het besluitvormingsproces van de standaard is toegankelijk voor iedereen die lid is van de OASIS Cyber Threat Intelligence Technical Committee. Iedereen kan lid worden. Het beheerproces voldoet ook overigens aan de eisen die het Forum stelt, zoals de mogelijkheid tot bezwaar, gepubliceerd beleid met betrekking tot versiebeheer en toegankelijke beheerdocumentatie.

De indiener raadt af het predicaat 'Uitstekend beheerproces' toe te kennen, doordat grote wijzigingen die doorgevoerd kunnen worden het wenselijk is om aanvullende toetsing plaats te laten vinden.

3.3 Draagvlak

Aanbieders en gebruikers moeten voldoende positieve ervaring met de standaard hebben.

3.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

3.3.1.1 *Bieden meerdere leveranciers ondersteuning voor de standaard?*
Ja, STIX en TAXII worden door de intrusion detection en threat intel markt gezien als 'de' standaarden. Leveranciers van oplossingen die STIX en TAXII ondersteunen zijn onder andere:

- Splunk
- HP ArcSight
- IBM QRadar
- Alienvault
- EclecticIQ
- ThreatConnect
- Anomali
- ThreatQuotient

3.3.1.2 *Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?*
Ja, er is open source tooling beschikbaar om validatie te doen. Zie bijvoorbeeld: https://github.com/STIXProject/stix-validator.

3.3.1.3 *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, de STIX standaard zorgt voor een gemeenschappelijk dataformaat en de TAXII standaard verzorgt het transport. Er is ruimte voor lokale aanpassingen met bijvoorbeeld eigen velden, maar de STIX standaard tracht dit overbodig te maken.

Met STIX en TAXII alleen is de interoperabiliteit nog niet gegarandeerd. STIX Profielen definiëren een subset van de STIX-objecten en attributen. Ze kunnen worden gebruikt om aan te geven dat slechts een subset van STIX wordt ondersteund of geproduceerd. Er is geen "de facto" STIX-profiel aan te wijzen. In beginsel staat een gebruiker de volledige STIX-

standaard ter beschikking, maar als er een beperkt aandachtsgebied is of met een incomplete STIX-implementatie wordt gewerkt, kan het zinvol zijn dit te beschrijven in een STIX profiel. Het is denkbaar dat als STIX binnen de overheid meer gebruikt gaat worden er STIX-profielen worden opgesteld en op elkaar worden afgestemd. Het is nu echter te vroeg om al een STIX overheidsprofiel op te stellen en voor te schrijven. De indiener adviseert dan ook om STIX 1.2.1 zonder beperkend STIX-profiel als standaard op te nemen, maar wel richtlijnen op te stellen voor het gebruik van de standaard.

3.3.1.4 Zijn er profielen of voorbeeldimplementaties van de standaard aanwezig en zijn deze vrij te gebruiken?
Ja, STIX 1.x heeft referentieprofielen. Zie http://stixproject.github.io/documentation/profiles/.

3.3.2 Kan de standaard rekenen op voldoende draagvlak?

3.3.2.1 Staan de belangrijkste stakeholders vanuit de overheid voor deze standaard achter de adoptie van de standaard?
Ja, STIX en TAXII zijn onder andere in gebruik bij:

- Belastingdienst
- Rijkswaterstaat
- SSC-ICT
- DUO
- Ministerie van Veiligheid & Justitie, inclusief NCSC

Alleen het NCSC verspreidt momenteel informatie via STIX en TAXII. De andere genoemde partijen halen informatie op met STIX en TAXII. Ook de andere partijen zullen later mogelijk informatie via STIX en TAXII gaan verspreiden.

De standaard is relevant voor alle (onderdelen) van overheden (Rijk, provincies en gemeenten) en instellingen uit de (semi-) publieke sector die in het kader van hun informatiebeveiliging gestructureerde dreigingsinformatie verzamelen en uitwisselen. Denk hierbij in het bijzonder aan Security Operations Centers.

3.3.2.2 Staan de overheidsorganisaties die daadwerkelijk worden geraakt door een mogelijke verplichting van de standaard achter het gebruik van de standaard?
Ja, zie paragraaf 3.3.2.1.

3.3.2.3 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?
Ja, zie paragraaf 3.3.2.1.

3.3.2.4 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?
Ja, versies STIX 1.2 en TAXII 1.1 zijn mogelijk ook nog in gebruik.

3.3.2.5 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?
Ja, STIX 1.2.1 en TAXII 1.1.1 zijn semantisch gelijk aan STIX 1.2 en TAXII 1.1.

3.3.2.6 *Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?*
Ja, er is steun vanuit de RijksISAC (Information Sharing and Analysis Center) waar veel partijen binnen de Rijksoverheid partij bij zijn, evenals de CTO-Raad van de Rijksoverheid. Veel leveranciers ondersteunen de standaard, zie 3.3.1.1.

3.3.3 Conclusie criteria 'Draagvlak'
De standaarden STIX en TAXII zijn inmiddels in gebruik bij het NCSC, de Belastingdienst, Rijkswaterstaat en SSC-ICT. De standaarden STIX en TAXII worden ondersteund door Splunk, HP ArcSight, IBM QRadar, Alienvault, EclecticIQ, ThreatConnect, Anomali en ThreatQuotient. Ook is er open source tooling beschikbaar om een implementatie te valideren.

De standaard is relevant voor alle overheidsorganisaties (Rijk, provincies, gemeenten) en instellingen in de (semi-) publieke sector die in het kader van hun informatiebeveiliging gestructureerde dreigingsinformatie verzamelen en uitwisselen. Denk hierbij in het bijzonder aan Security Operations Centers. De CTO-Raad van de Rijksoverheid, het RijkISAC en de IBD Gemeenten ondersteunen expliciet de aanmelding van deze standaard bij het Forum Standaardisatie.

3.4 Opname bevordert adoptie

De opname op de lijst is een geschikt middel om de adoptie van de standaard te bevorderen.

Met de lijst wil het Nationaal Beraad de adoptie van open standaarden bevorderen die voldoen aan de voorgaande criteria (toegevoegde waarde, standaardisatieproces en draagvlak).
- Met de "pas toe of leg uit"-status beoogt het Nationaal Beraad standaarden te verplichten als:
  a. hun huidige adoptie binnen de (semi-)overheid beperkt is;
  b. opname op de lijst bijdraagt aan de adoptie door te stimuleren (functie = stimuleren).
- Met de aanbevolen standaarden beoogt het Nationaal Beraad standaarden aan te bevelen als :
  a. hun huidige adoptie binnen de (semi-)overheid reeds hoog is;
  b. opname op de lijst bijdraagt aan de adoptie door te informeren en daarmee onbedoelde afwijkende keuzes te voorkomen (functie = informeren).

3.4.1 Is "pas toe of leg uit" het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Het geautomatiseerd delen van dreigingsinformatie (binnen de overheid) staat nog aan het begin, evenals de adoptie van standaarden voor deze gegevensuitwisseling. Het plaatsen van de STIX- en TAXII-standaarden op de lijst open standaarden stimuleert het gebruik van deze standaarden en zal zo zorgen voor betere interoperabiliteit. Er ontstaat momentum voor de standaarden en opname als verplichte standaard (pas-toe-of-leg-uit) op de lijst open standaarden kan dit momentum vergroten.

3.4.2 Is de status "aanbevolen" het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Nee, de adoptie van de standaard is niet hoog en er is nog geen grote staande praktijk van het geautomatiseerd uitwisselen van dreigingsinformatie.

3.4.3 Conclusie criteria 'Opname bevordert adoptie'

De experts adviseren het Forum Standaardisatie de standaarden STIX en TAXII op te nemen op de lijst open standaarden met de status 'pas toe of leg uit'.

3.5 Adoptieactiviteiten

Gebruik van de standaard is het einddoel van het Forum Standaardisatie en Nationaal Beraad. Plaatsing op de lijst met open standaarden is hiervoor een goede stap, maar voor het daadwerkelijk adopteren (implementeren en gebruiken) van de standaard is vaak aanvullende actie benodigd. Aanvullend kan Forum Standaardisatie dan ook bijdragen aan adoptie van de standaard door het actief inzetten van adoptie-instrumenten of ondersteunende acties. Welke kansen zijn er om de adoptie te versnellen en welke drempels bestaan er die de adoptie van de standaard hinderen?

De expertgroep adviseert het Nationaal Beraad om bij de opname op de lijst voor 'pas toe of leg uit' de volgende oproepen ten aanzien van de adoptie van STIX en TAXII te doen:

- Het Forum roept het NCSC op om samen met betrokkenen een leidraad op te stellen, al dan niet als onderdeel van een bestaand kennisproduct[3], 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.
- Het Forum 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.
- Het Forum 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.
- Het Forum roept overheden die STIX en TAXII toepassen op om informatie over de meerwaarde van het gebruik voor hen en *best practices* te delen.
- Het Forum roept KING op om in de GGI (gemeentelijke gemeenschappelijke infrastructuur) STIX en TAXII toe te passen in het SOC (security operations center).

De expertgroep adviseert het Forum Standaardisatie de adoptie en deze oproepen na 2 jaar te evalueren.

[3] *Het NCSC en de AIVD hebben reeds een whitepaper over dit vraagstuk uitgebracht (zie https://www.ncsc.nl/actueel/whitepapers/handreiking-voor-implementatie-van-detectie-oplossingen.html). Daarnaast heeft het NCSC een factsheet over Indicators of Compromise uitgegeven (zie https://www.ncsc.nl/actueel/factsheets/factsheet-indicators-of-compromise.html).*