Intakeadvies STIX en TAXII 2.1

Vergadering:	Forum Standaardisatie woensdag 24 september 2025
Agendapunt:	
Documentnummer:	
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	29 augustus 2025
Versie:	0.9
Bijlagen:	geen
Rechten:	CC0 publieke domein verklaring

1 Samenvatting en advies

De Stuurgroep Open Standaarden adviseert het Forum Standaardisatie om de nieuwe versies (beide versie 2.1) van Structured Threat Information Expression (STIX) en Trusted Automated eXchange of Indicator Information (TAXII), in samenhang in procedure te nemen voor opname op de 'Pas toe of leg uit'-lijst. Een volledig expertonderzoek is aangewezen om de standaarden te toetsen aan de criteria voor opname op de 'Pas toe of leg uit'-lijst. Deze standaarden, doorgaans in combinatie gebruikt, gelden binnen de markt voor cyberindringingsdetectie en dreigingsinformatie in versie 2.1 als de toonaangevende standaarden. 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 intakeadvies 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 dat zich richt op de ontwikkeling en adoptie van open standaarden voor informatie-uitwisseling.

Indien het Forum Standaardisatie besluit tot het in procedure nemen van STIX en TAXII versie 2.1, dan kan tijdens de expertbijeenkomst en bij het tot stand komen van het expertadvies extra aandacht worden besteed aan de volgende punten:

- Aandacht voor mogelijke wetgeving die verplichtingen oplegt voor het delen van cyber security informatie;
- Aandacht voor het belang van de maatschappelijke waarde van de standaard;
- Aandacht voor de regierol van het NCSC in Nederland met betrekking tot STIX en TAXII versie 2.1;
- Aandacht voor het verkennen van de toepassing van STIX en TAXII versie 2.1 bij gemeenten en waterschappen.

In de rest van dit document wordt het advies nader onderbouwd. Hoofdstuk 2 geeft een korte uitleg van de standaarden. Hoofdstuk 3 beschrijft het proces waarmee dit advies tot stand kwam, alsmede de vervolgstappen. Hoofdstuk 4 toetst in hoeverre de standaard voldoet aan de criteria om in behandeling genomen te worden door het Forum Standaardisatie. Hoofdstuk 5 verkent of er inhoudelijke belemmeringen bestaan die een positief expertadvies in de weg zouden kunnen staan. Tenslotte wordt er in hoofdstuk 6 een praktijkvoorbeeld gegeven dat Forum Standaardisatie kan gebruiken om de maatschappelijke waarde van de standaard te communiceren.

2 Korte beschrijving van de standaard

2.1 Over de standaard

STIX draagt bij aan het consistent delen, opslaan en analyseren van cyberdreigingsinformatie. Het biedt een datamodel om informatie over cyberbedreigingen uit te wisselen op een manier die zowel mensen als machines kunnen begrijpen. STIX is relevant voor iedereen die betrokken is bij cyberdefense, inclusief analisten van cyberbedreigingen, malware-analisten, leveranciers van beveiligingstools, beveiligingsonderzoekers en gemeenschappen die bedreigingen delen.

TAXII draagt bij aan het geautomatiseerd en real-time uitwisselen van cyberdreigingsinformatie. Het biedt een toepassingsprotocol voor het uitwisselen en communiceren van cyberdreigingsinformatie op een eenvoudige en schaalbare manier. TAXII definieert concepten, protocollen en berichten om informatie over cyberbedreigingen uit te wisselen voor de detectie, preventie en beperking van cyberbedreigingen. TAXII stelt organisaties in staat om zicht te krijgen op komende dreigingen. Ook stelt het organisaties in staat om de informatie gemakkelijk te delen met partners. TAXII is speciaal ontworpen om de uitwisseling van cyberdreigingsinformatie te ondersteunen die in STIX wordt vertegenwoordigd. Ondersteuning voor het uitwisselen van STIX-inhoud is een standaard onderdeel van TAXII. TAXII kan echter ook worden gebruikt om gegevens in andere formaten te delen. Het is belangrijk op te merken dat STIX en TAXII onafhankelijke standaarden zijn: de structuren en serialisaties van STIX zijn niet afhankelijk van een specifiek transportmechanisme en TAXII kan worden gebruikt om niet-STIX-gegevens te transporteren.

2.2 Waarom is deze standaard belangrijk?

STIX heeft een belangrijke rol voor goede informatie-uitwisseling van cyberdreigingsinformatie, doordat het een consistent, gestructureerd en machineleesbaar formaat biedt om indicatoren, incidenten en dreigingsactoren eenduidig te beschrijven en delen. TAXII is ontworpen om de uitwisseling te ondersteunen van cyberdreigingsinformatie die in STIX wordt vertegenwoordigd. Door deze standaarden te implementeren zijn organisaties snel op de hoogte van cyberdreigingen. 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 geautomatiseerd delen van dreigingsinformatie (binnen de overheid). Veel organisaties, waaronder NCSC, gebruiken reeds versie 2.1. De facto loopt de 'Pas toe of leg uit'-status van STIX versie 1.2.1 en TAXII versie 1.1.1 achter op de dagelijkse praktijk.

STIX en TAXII versie 2.1 bieden ten opzichte van de vorige versies meerwaarde. De standaarden zijn verbeterd op meerdere punten. 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 toeziet op cybersecurity in Europa 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 en het uitwisselen van dreigingsinformatie onnodig ingewikkeld. Daarom heeft de CTI TC voor versie 2.1 het datamodel en de opslagmethode herzien, en 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. Inmiddels gelden de versies 2.1 als de facto standaarden voor het uitwisselen van cyberdreigingsinformatie. De oudere 1.*-versies gelden als verouderd, omdat deze in zeer beperkte mate worden 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. STIXX 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.

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 cyberdreigingen uit te wisselen. Door deze wettelijke verplichtingen en mandaten zal er meer cyberdreigingsinformatie worden gedeeld. Zonder standaardisatie kan deze informatie niet effectief en tijdig worden gebruikt om cyberdreigingen te detecteren. Dit benadrukt het belang van uniforme standaarden voor een effectieve en veilige informatie-uitwisseling.

3 Betrokkenen en proces

Op 15 april 2025 heeft het Nationaal Cyber Security Centrum (NCSC) STIX en TAXII versie 2.1 aangemeld om te toetsen of de standaarden in de nieuwe versie geschikt zijn om te blijven verplichten (‘Pas toe of leg uit’) aan de overheid.

Op 20 mei 2025 heeft een intakegesprek plaatsgevonden met de indiener, procedurebegeleider InnoValor Advies en Bureau Forum Standaardisatie. Bij dit online intakegesprek waren de volgende personen aanwezig:

- Luitzen Homma (NCSC - Indiener)
- Luuk Matthijssen (NCSC - Indiener)
- Aday Destici (InnoValor Advies)
- Koen de Jong (InnoValor Advies)
- Bart Knubben (Bureau Forum Standaardisatie)
- Wouter Kobes (Bureau Forum Standaardisatie)
- Joram Verspaget (Bureau Forum Standaardisatie)

In dit gesprek is onderzocht of STIX en TAXII versie 2.1 voldoet aan de criteria om in procedure te worden genomen. Daarnaast is vooruitgeblikt op de procedure. Dit intakeadvies is tot stand gekomen op basis van het intakeonderzoek.

4 Voldoet de standaard aan de criteria om in procedure te worden genomen?

STIX en TAXII versie 2.1 voldoen aan alle vier criteria om in behandeling genomen te worden voor plaatsing op de 'Pas toe of leg uit'-lijst. Hoe de standaarden zijn getoetst op de vier criteria wordt hieronder toegelicht in paragrafen 4.1-4.4.

4.1 Valt de standaard binnen de scope van Forum Standaardisatie?

Criterium: "Het opnemen van de standaard op de lijst dient in substantiële mate bij te dragen aan het bevorderen van de interoperabiliteit, van een toekomstbestendige gegevensopslag en/of van een verminderde leveranciersafhankelijkheid."

Ja, de standaarden STIX en TAXII vallen binnen de scope van het Forum Standaardisatie. De standaarden STIX en TAXII staan reeds tezamen onder één registratie op de 'Pas toe of leg uit'-lijst en zijn toepasbaar voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling. Hoewel de standaarden in theorie ook kunnen worden gebruikt voor communicatie tussen overheidsorganisaties en burgers, is dit minder gebruikelijk. Dit omdat STIX en TAXII versie 2.1 zich richten op technische en gedetailleerde informatie over cyberdreigingen, wat meestal relevant is voor organisaties met gespecialiseerde security afdeling(en) met een hoog cybervolwassenheidsniveau.

4.2 Heeft de standaard een toepassing die binnen de overheid een enkele organisatie of sector overstijgt?

Criterium: "Het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard dient voldoende breed te zijn en betrekking te hebben op gebruik door de (semi-)overheid."

Ja, de standaard heeft een toepassing die binnen de overheid een enkele organisatie of sector overstijgt. Het functioneel toepassingsgebied en het organisatorisch werkingsgebied van STIX en TAXII zijn en blijven voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid. De nieuwe versies (versie 2.1) brengen hier geen verandering in. De standaarden zijn ontworpen om samenwerking tussen verschillende organisaties (commerciële en open source implementaties) te ondersteunen, wat essentieel is voor een gecoördineerde aanpak van cyberdreigingen. Dit omvat samenwerking tussen overheidsinstanties onderling, maar ook tussen overheidsinstanties en private sectoren.

4.3 Is de standaard niet al wettelijk verplicht?

Criterium: "Het uitvragen of gebruiken van de standaard moet niet al verplicht zijn op grond van een bestaande (Europees) wettelijke verplichting die gelijk dan wel groter is dan het voor de lijst beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied."

Ja, de standaard is niet al wettelijk verplicht. Met de Cyberbeveiligingswet (CBW) komt er vernieuwde wetgeving aan die bedrijven in vele sectoren verplicht over cybersecurity-informatie te delen, waardoor de vrijblijvendheid verdwijnt en concrete verplichtingen gelden. De CBW zal naar verwachting het tweede kwartaal van 2026 in werking treden als opvolger van de Wet beveiliging netwerk- en informatiesystemen (Wbni) en implementeert de bredere verplichtingen uit de NIS2 richtlijn in Nederland. Ook de Wet Bevordering Digitale Weerbaarheid Bedrijven (Wbdwb) heeft een rol in het delen van dreigingsinformatie. Deze geeft de minister van Economische Zaken en het Digital Trust Center het wettelijk mandaat om de digitale weerbaarheid van bedrijven in Nederland te versterken. Het doel is om Nederland beter weerbaar te maken tegen cyberdreigingen. Zowel de CBW als de Wbdwb verplichten het gebruik van STIX en TAXII versie 2.1 niet, maar zullen door de verplichting tot het delen van dreigingsinformatie wel bijdragen aan de adoptie ervan.

4.4 Draagt de standaard bij tot de oplossing van een bestaand, relevant probleem?

Criterium: “De standaard dient bij te dragen aan de oplossing van een bestaand, relevant probleem.”

Ja, de standaard draagt bij aan de oplossing van een bestaand, relevant en welomschreven (interoperabiliteits)probleem en het voorkomen van leveranciersafhankelijkheid. In het cyberlandschap gebruiken veel applicaties zelf ontwikkelde implementaties voor het verwerken van dreigingsinformatie. Dit maakt het uitwisselen van dreigingsinformatie tussen applicaties complex. 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. Ook het NCSC gebruikt de standaard om dreigingsinformatie met haar doelgroep te delen. STIX en TAXII versie 2.1 bieden standaarden waarmee organisaties op een gestructureerde en geautomatiseerde wijze informatie over cyberdreigingen kunnen uitwisselen. Het uitwisselen van dreigingsinformatie draagt bij aan de weerbaarheid tegen cyberaanvallen. Binnen het domein van cyberveiligheid is snelheid cruciaal. Wanneer informatie niet op een uniforme, machine-to-machine (M2M) manier wordt gedeeld, is tijdige reactie op dreigingen zeer uitdagend. Daarom is het van strategisch belang om deze uitwisseling interoperabel te maken. De standaarden STIX en TAXII dragen hieraan bij.

5 Is er zicht op een positief expertadvies?

Ja, er is zicht op een positief expertadvies. Het intakeonderzoek heeft geen inhoudelijke bezwaren opgeleverd die een positief expertadvies voor plaatsing van STIX en TAXII versie 2.1 op de ’Pas toe of leg uit’-lijst in de weg zouden kunnen staan.

Als het Forum Standaardisatie de standaard in procedure neemt, wordt een groep experts gevraagd de standaard te toetsen op de vier inhoudelijke hoofdcriteria voor opname op de ‘Pas toe of leg uit’-lijst of de lijst aanbevolen standaarden. Het Forum Standaardisatie neemt geen standaarden in procedure waarvan bij aanvang al vaststaat dat deze niet op een positief

expertadvies kunnen rekenen. Daarom wordt in dit intakeadvies vooruitgeblikt op de vier inhoudelijke hoofdcriteria. Dit wordt toegelicht in paragrafen 5.1-5.4.

5.1 Toegevoegde waarde

Er zijn geen conflicterende standaarden voor het delen van bruikbare informatie over cyberdreigingen vastgelegd door het Forum Standaardisatie. STIX versie 2.1 biedt meer flexibiliteit en TAXII versie 2.1 maakt het delen van bruikbare informatie over cyberdreigingen mogelijk over organisatie- en product-/service grenzen heen. De nieuwe versies van de standaarden zijn beter toepasbaar in operationele processen. Door de toegenomen detaillering maken de standaarden het eenvoudiger om te interpreteren waar de data over gaat. Hierdoor ontstaat de mogelijkheid om specifieke dreigingsinformatie uit te wisselen.

De grotere gedetailleerdheid kan echter ook voor meer complexiteit zorgen, wat de adoptie van de nieuwe versies kan vertragen (Evaluatie cluster 'Veilig Internet'). Deze complexiteit ligt met name in de hoeveelheid cyberdreigingsinformatie die met STIX en TAXII kan worden uitgewisseld. Het verkrijgen van inzichten uit grote hoeveelheden ruwe data vereist specialistische analyse. Data-analisten gebruiken hun technische expertise om dreigingsbeelden te genereren uit de beschikbare informatie. Hiermee ondersteunen zij het werken aan oplossingen op strategisch, tactisch en operationeel niveau.

Aan de adoptie van de standaarden zijn niet direct kosten verbonden. De kwalitatieve en kwantitatieve voordelen van de adoptie wegen op tegen de nadelen. Deze voordelen omvatten onder andere:

1. *Geen directe kosten voor adoptie:* STIX en TAXII versie 2.1 zijn open standaarden, beheerd door OASIS, en vrij beschikbaar zonder licentiekosten. Er zijn meerdere open source libraries beschikbaar die adoptie mogelijk maken zonder dure commerciële software.
2. *Kwalitatieve voordelen*: STIX en TAXII maken gestandaardiseerde uitwisseling van dreigingsinformatie mogelijk tussen organisaties, sectoren en tools. STIX dwingt een gestructureerde manier van denken af over dreigingen wat de kwaliteit van dreigingsanalyse verbetert.
3. *Kwantitatieve voordelen:* Door automatisering van informatie-uitwisseling en verwerking hoeven analisten minder handmatig te werken. Geautomatiseerde indicatorverwerking maakt snellere detectie van bedreigingen mogelijk.
4. *De nadelen wegen niet op tegen de voordelen:* Bij de eerste implementatie is er enige complexiteit in het leren werken met STIX-objecten en TAXII-endpoints. Initieel moet er worden geïnvesteerd, maar dit is eenmalig en beperkt in verhouding tot de structurele voordelen.

De standaard stelt organisaties in staat eenvoudiger en efficiënter dreigingsinformatie met elkaar uit te wisselen. Daarmee ligt de (kwalitatieve) business case vooral in het verkleinen van de kans op succesvolle cyberaanvallen en -incidenten. STIX en TAXII vormen op zichzelf

geen beveiligingsrisico, maar een onveilige implementatie of onjuist gebruik kan wel risico's introduceren. Mogelijke gevaren zijn het automatisch verwerken van onbetrouwbare dreigingsinformatie, het onbedoeld delen van gevoelige data, 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. Wat betreft privacyrisico's geldt dat STIX en TAXII 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.

5.2 Open standaardisatieproces

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. Daarnaast is de documentatie over het ontwikkel- en beheerproces van STIX en TAXII versie 2.1 eveneens publiek beschikbaar via de OASIS-website. 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. De standaardisatieorganisatie garandeert dat partijen die bijdragen aan de ontwikkeling van de standaarden hun intellectueel eigendomsrecht onherroepelijk royalty-free voor eenieder beschikbaar stellen. OASIS (Organization for the Advancement of Structured Information Standards) 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.

Het besluitvormingsproces is toegankelijk voor alle belanghebbenden, waaronder gebruikers, leveranciers, adviseurs en wetenschappers. OASIS biedt hiervoor verschillende mogelijkheden. OASIS houdt rekening met verschillende belangen door een transparant en inclusief proces te hanteren waarbij diverse belanghebbenden kunnen deelnemen en input kunnen geven. Belanghebbenden kunnen formeel bezwaar aantekenen tegen de gevolgde procedure. Daarnaast organiseert OASIS regelmatig overleggen met belanghebbenden over de doorontwikkeling en het beheer van de standaard. Voorafgaand aan de vaststelling van een nieuwe versie van de standaard organiseert OASIS een publieke consultatie. 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.

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.

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. 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. Het is aan het Forum om te bepalen of aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard noodzakelijk is. 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 wenselijk dat een nationale regierol voor de standaarden wordt ingevuld. OASIS Open fungeert als aanspreekpunt waar meer informatie over de standaarden beschikbaar is. Ook kan de OASIS community hiervoor worden benaderd.

5.3 Draagvlak

De belangrijkste stakeholders vanuit de overheid staan achter de adoptie van de standaarden. Zie ook de Evaluatie cluster 'Veilig Internet' en pagina 17-20 van de inventarisatie gebruiksgegevens 2024. 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. 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 cyberdreigingsinlichtingen data willen uitwisselen met het NCSC. Uit de Evaluatie cluster 'Veilig Internet' blijkt echter dat adoptie bij gemeenten en waterschappen achterblijft. 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. De aangemelde versie 2.1 is niet backwards compatible met eerdere versies van de standaarden. Er zijn voldoende positieve signalen over huidig en toekomstig gebruik van de standaarden door (semi-)overheidsorganisaties, het bedrijfsleven en burgers. Zie hierover het evaluatierapport.

Meerdere leveranciers bieden ondersteuning en het zijn breed geaccepteerde standaarden voor het delen 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 open source 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. Er zijn diverse tools beschikbaar waarmee getest kan worden of een koppeling correct functioneert. Het beschikbaar stellen van een API-endpoint maakt geautomatiseerde testen mogelijk. Daarnaast biedt OASIS verschillende ondersteunende tools aan via hun website. Ook is er open source tooling beschikbaar voor validatie.

5.4 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. NCSC geeft invulling aan haar rol voor de uitwisseling 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 te 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.

6 Praktijkvoorbeeld

Het Nationaal Cyber Security Centrum (NCSC) heeft vanuit wetgeving de taak om organisaties binnen haar doelgroep, waaronder Rijksoverheidsorganisaties en NIS2-organisaties, adequaat te informeren over cyberdreigingen. 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. Later dit jaar zal deze informatievoorziening worden uitgebreid naar de NIS2-doelgroep. 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 later dit jaar (2025) automatisch waargenomen dreigingen, zogenaamde sightings, rapporteren aan het NCSC via dezelfde STIXX 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. De bredere uitrol staat gepland voor later dit jaar (2025).