FS-20221207.3C2

Evaluatie cluster 'Veilig internet'

Evaluatie standaarden STIX en TAXII

InnoValor Advies

Colofon

Projectnaam	Evaluatie standaarden 2022
Auteurs	M. Roelfsema (InnoValor)
	L. Hijink (InnoValor)
Opdrachtgever	Forum Standaardisatie
	Postbus 96810
	2509 JE Den Haag
	info@forumstandaardisatie.nl
	Forum Standaardisatie

Inhoudsopgave

1. Inleiding

1.1. Achtergrond

Forum Standaardisatie is een onafhankelijke overheidsorganisatie die de overheid adviseert over het gebruik van open ICT standaarden in de digitale overheid. Open standaarden zorgen voor een betere uitwisselbaarheid en toegankelijkheid van gegevens. Forum Standaardisatie zorgt ervoor dat digitale gegevens veiliger en gemakkelijker met elkaar uitgewisseld kunnen worden. Zo helpen zij de samenwerking binnen de publieke sector te verbeteren. In opdracht van het Forum Standaardisatie voert Bureau Forum Standaardisatie (BFS) initiatieven uit om het gebruik van open standaarden bij de overheid te bevorderen.

Een van de manieren van Forum Standaardisatie om de onderlinge samenwerking van overheden te bevorderen is door open standaarden te toetsen en voor te schrijven aan publieke organisaties. Op de 'pas toe of leg uit'-lijst (verplichte standaarden) van het Forum Standaardisatie staan standaarden die overheden verplicht moeten toepassen volgens 'pas toe of leg uit'-verplichting op het moment dat ze een ICT-dienst of -product aanschaffen dat binnen het desbetreffende toepassingsgebied valt van de standaard.

De 'pas toe of leg uit'-lijst wordt onderhouden op basis van een open procedure. De toetsing bij aanmelding is een momentopname. Als een standaard een aantal jaar op de 'pas toe of leg uit'-lijst staat, kan het zijn dat de relevantie, het draagvlak, het toepassingsgebied of de marktpartijen veranderd zijn. Er kunnen dan vragen ontstaan als: Heeft de standaard nog toegevoegde waarde? Wordt de standaard nog door voldoende marktpartijen ondersteund?

In zulke gevallen kan het Forum Standaardisatie besluiten om standaarden te evalueren. Dit gaat dan om standaarden die langer dan vier jaar of langer op de lijst 'pas toe of leg uit'-lijst staan. Voor 2022 evalueert het Forum Standaardisatie twee standaarden uit het domein 'Veilig internet', ook wel bekend als het domein 'Internet en Beveiliging', in dit rapport hanteren we de nieuwe benaming 'Veilig internet'. Het gaat om STIX en TAXII. De evaluatie brengt de samenhang van de twee standaarden in beeld. Dit draagt bij aan duiding van de standaarden op maatschappelijke meerwaarde.

1.2. Leeswijzer

De evaluaties van STIX en van TAXII zijn in een document samengebracht. Hoofdstuk 1 biedt achtergrond, een toelichting, het doel en de aanpak van beide evaluaties. Hoofdstuk 2 toont de evaluatie van STIX en Hoofdstuk 3 geeft de evaluatie van TAXII weer.

De STIX en TAXII standaarden worden doorgaans in combinatie gebruikt. Op de 'pas toe of leg uit'-lijst staan beide standaarden nu als één standaard opgenomen. Het doel van deze evaluatie is om beide standaarden afzonderlijk te evalueren en in dit document zijn beide evaluaties afzonderlijk te lezen. De opgehaalde informatie en inzichten zijn echter voor beide standaarden relevant. Om die reden zit er veel tekstuele overlap tussen hoofdstuk 2 en hoofdstuk 3.

Hoofdstuk 2 en 3 kennen een vergelijkbare opbouw:

- Inleiding
    - Toelichting op de standaard
    - De betrokken experts
- Evaluatie

    - Toepassingsgebied
    - Toegevoegde waarde
    - Draagvlak
    - Beheer
    - Impact opname op de lijst
    - Status adoptieadviezen
    - Lopende ontwikkelingen
- Conclusies en aanbevelingen

Hoofdstuk 4 geeft een algemene conclusie aan aanbevelingen die betrekking hebben op het cluster ‘Veilig internet’.

1.3. Vraagstelling en doel

Het Bureau Forum Standaardisatie heeft de opdracht gegeven om twee standaarden vanuit het domein ‘Veilig internet’, die op de ‘Pas toe of leg uit’-lijst staan te evalueren: STIX en TAXII.

Dit rapport is het resultaat van de evaluatie. Hieronder een korte toelichting per standaard en de reden voor evaluatie.

STIX draagt bij aan veilig internet doordat cyberdreigingsinformatie gemakkelijker en sneller uit te wisselen is waardoor geautomatiseerde detectie van en reactie op cyberdreigingen mogelijk wordt. STIX wordt gebruikt voor het consistent delen, opslaan en analyseren van cyberdreigingsinformatie doordat het een gestructureerde taal biedt om informatie over cyberdreigingen uit te wisselen. STIX stelt organisaties via tools in staat dreigingsinformatie met elkaar te delen. Dit biedt allerlei mogelijkheden, zoals gezamenlijke dreigingsanalyse, geautomatiseerde uitwisseling van dreigingen, geautomatiseerde detectie en reactie, en meer. Op 10 juni 2021 is een nieuwe versie van STIX, namelijk STIX 2.1, goedgekeurd door de leden van OASIS (beheerorganisatie). Een nieuwe versie maak het relevant om de standaard op de ‘pas toe of leg uit’-lijst te evalueren. Het NCSC adviseert inmiddels STIX versie 2.1 bij aanschaf van nieuwe cybersecurity software. Dit loopt uit de pas met versie 1.2.1. van STIX die op de ‘pas toe of leg uit’-lijst staat.

TAXII draagt bij aan veilig internet doordat het real-time uitwisselen van cyberdreigingsinformatie mogelijk maakt wat de reactietijd van organisaties op cyberdreigingen aanzienlijk kan versnellen. TAXII staat voor het geautomatiseerd en in real-time uitwisselen van cyberdreigingsinformatie doordat het een protocol biedt voor de communicatie van cyberdreigingsinformatie op een eenvoudige en schaalbare manier. TAXII is specifiek ontworpen voor de uitwisseling van cyberdreigingsinformatie in STIX-formaat, maar is niet beperkt tot STIX. STIX valt daarnaast uit te wisselen met vele andere protocollen dan TAXII, denk aan SCP, FTP en HTTPS, ieder transport protocol kan werken. Op 10 juni 2021 is een nieuwe versie van TAXII, namelijk TAXII 2.1, goedgekeurd door de leden van OASIS (beheerorganisatie). Een nieuwe versie maak het relevant om de standaard op de ‘pas toe of leg uit’-lijst te evalueren.

In het Forumadvies d.d. 19 september 2017 is opgenomen dat de expertgroep het Forum Standaardisatie destijds heeft geadviseerd om de adoptie van STIX 1.2.1 en TAXII 1.1.1 en de oproepen daaromtrent na twee jaar te evalueren. Inmiddels is dit vijf jaar geleden. Daarnaast heeft het Forum Standaardisatie het advies gegeven aan meerdere partijen om kennis en ervaringen uit te wisselen, en om de meerwaarde van deze standaard te beoordelen. Vijf jaar na opname op de ‘pas toe of leg uit’- lijst is het relevant om te bekijken in hoeverre dit is gelukt.

1.4. Aanpak

Voorafgaand aan de evaluatie is er een kick-off geweest tussen de procesbegeleiders van InnoValor (Melissa Roelfsema en Liesbeth Hijink) en de opdrachtgever (Hans Laagland namens Bureau Forum Standaardisatie). Tijdens deze kick-off is de werkwijze van de evaluatie aan bod gekomen en is er een eerste aanzet gemaakt tot een lijst van experts en potentiële interviewkandidaten. Het doel is om de beheerder, gebruikers en leveranciers te spreken die elk een ander aspect van de standaard kan belichten. Daaropvolgend is er een gesprek geweest met de dossierhouders veilig internet Bart Knubben en Robin Gelhard (Bureau Forum Standaardisatie), waarin de werkwijze nogmaals is toegelicht en de lijst met interviewkandidaten is aangescherpt. Vanuit de lijst zijn er verschillende experts benaderd met het verzoek tot een semigestructureerd interview. Tijdens dit gesprek zijn beide standaarden en de stand van zaken toegelicht door de dossierhouders.

Tijdens het opstellen van de lijst met experts bleek al snel dat er geen experts specifiek vielen aan te wijzen voor een van de twee standaarden, maar dat beide standaarden toch vaak in combinatie ingezet worden. Hierdoor is er besloten om de interviews met experts in te steken op beide standaarden met daarin aandacht in het interview voor elke standaard afzonderlijk.

Op basis van de aanscherping is er contact gezocht met de experts voor semigestructureerde interviews omtrent de standaarden. De resultaten van de interviews zijn, waar relevant, verwerkt in dit rapport. De uitwerking van de evaluatie is gedeeld met dossierhouders en opdrachtgever ter review. Na review is er besloten om aanvullende interviews te houden om extra verdieping te geven daar waar nodig.

1.4.1. Evaluatiecriteria

De evaluatie van de standaarden heeft plaatsgevonden op basis van de volgende criteria:

1. Is het functioneel toepassingsgebied nog juist? Is dit duidelijk en concreet geformuleerd, en in lijn met de criteria zoals toegepast in de Toets ideaaltypische syntactische structuur? Weet een potentiële gebruiker wanneer de standaard van toepassing is?

2. De toegevoegde waarde van de standaard. Heeft de standaard nog toegevoegde waarde? Welk reëel en als zodanig ervaren probleem heeft het opgelost?

3. Is er nog voldoende draagvlak voor de standaard? Hoe staat het met gebruik van de standaard, waar wordt deze toegepast binnen de overheid en wat zijn de toekomstige ontwikkelingen? Zijn er voldoende marktpartijen die het ondersteunen?

4. Voldoet het beheer en doorontwikkeling aan de vereiste criteria? Zijn er zaken veranderd in het beheer van de standaard sinds de plaatsing op de ‘Pas toe of leg uit’-lijst? Voldoet het beheer van de standaard nog aan de criteria voor openheid en is het besluitvormingsproces nog goed en actueel gedocumenteerd? Is de beheerder van de standaard nog actief?

5. Heeft opname op de lijst de adoptie bevorderd? Ondersteunen de experts de opname van de standaard op de ‘Pas toe of leg uit’-lijst? Wat zijn eventuele redenen om dit niet te ondersteunen? Wat zijn redenen om de standaard wel op de lijst te houden?

6. Zijn de adoptie adviezen opgevolgd? Bij verschillende standaarden zijn opname-adviezen meegegeven door het Forum om de adoptie te bevorderen. Zijn deze adviezen opgevolgd en/of zijn er nieuwe adoptie adviezen mee te geven?

7. Zijn er relevante lopende ontwikkelingen? Wat zijn de toekomstige ontwikkelingen met betrekking tot de standaard (of gerelateerde standaarden) en het interoperabiliteitsprobleem dat het oplost? Heeft dit impact voor de positie van de standaard op de lijst? Zijn er nieuwe versies nieuwe standaarden op komst, is er een noodzaak tot verplicht gebruik hiervan, en is deze mogelijk geschikt voor opname op de lijst?

2. Evaluatie STIX

2.1. Inleiding

2.1.1. Toelichting STIX standaard

De Structured Threat Information Expression (STIX) draagt bij aan het consistent delen, opslaan en analyseren van cyberdreigingsinformatie doordat het een gestructureerde taal biedt 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 cyberdefensie, inclusief analisten van cyberbedreigingen, malware-analisten, leveranciers van beveiligingstools, beveiligingsonderzoekers en gemeenschappen die bedreigingen delen.

STIX is het resultaat van een gezamenlijke, door de gemeenschap aangestuurde inspanning om een raamwerk te definiëren en te ontwikkelen voor het uiten van informatie over cyberbedreigingen om het delen van cyberbedreigingsinformatie en analyse van cyberbedreigingen mogelijk te maken, meer informatie is beschikbaar bij OASIS. Het doel van de Structured Threat Information Expression (STIXTM)-inspanning is het specificeren, karakteriseren en vastleggen van informatie over cyberdreigingen. STIX richt zich op een volledige reeks van cyberdreigingen, waaronder dreigingsanalyse, vastlegging en specificatie van indicatoren, beheer van responsactiviteiten en het delen van informatie, om de consistentie, efficiëntie, interoperabiliteit en algemeen situationeel bewustzijn te verbeteren.

STIX concepten worden onder andere gebruikt in de use-case waarin een Threat Actor profiel geïdentificeerd wordt. Een Threat Actor is een persoon of groep die actie ondernemen waarbij het doel is om schade aan te brengen in de cyberwereld, waaronder computers, apparaten, systemen of netwerken. Threat Actors hebben waarneembare kenmerken zoals aliassen, doelen en motivaties die vastgelegd kunnen worden in een STIX object.

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.

Verschil STIX 1.x en STIX 2.x

Op de ‘pas toe of leg uit’-lijst is STIX 1.2.1 opgenomen. Inmiddels is STIX 2.1 uitgebracht. De verschillen tussen STIX 2.x en STIX 1.x zijn samen te vatten tot de volgende punten:

- STIX 1.x is gedefinieerd met XML. STIX 2.x vereist implementaties waarin JSON ondersteund wordt. JSON is lichter en werkt voldoende om informatie over cyberdreigingsinformatie over te brengen. Doordat JSON eenvoudiger te gebruiken is krijgt het steeds meer de voorkeur van ontwikkelaars.
- Alle objecten in STIX 2.x bevinden zich op het top-level, anders dan STIX 1.x waar objecten in andere objecten ingebed kunnen zijn.
- STIX 2.x introduceert een top-level STIX Relatie Object (SRO), waarmee twee objecten aan elkaar verbonden worden via een relatietype. In STIX 1.x werden relaties ingebed in andere objecten. De soorten relaties werden beperkt door de STIX 1.x specificatie, doordat relaties zelf geen object waren kon er geen relatie tussen twee objecten worden uitgedrukt zonder een van de objecten te wijzigen. Met het nieuwe relatie object kunnen anderen, naast de content ontwikkelaar, kennis toevoegen op een onafhankelijke manier.

- STIX 2.x beperkt het aantal objecten en eigenschappen tot een kernset van functies.
- STIX 2.x maakt niet meer gebruik van een specifieke taal voor seralisatie, zoals XPath.
- STIX 2.x specificeert een taal voor patronen die onafhankelijk is van de serialisatietaal. De patronen zijn compacter en gemakkelijker te lezen. Bovendien is er geen verwarring tussen patronen en waarnemen.

Kortom, STIX 2.x kent meer flexibiliteit en stelt de gebruiker in staat om kennis te verrijken waardoor het een stuk langer bruikbaar zal blijven.

Er is geen directe achterwaartse compatibiliteit tussen STIX 2.x en STIX 1.x. Er zijn allerlei open source tools die ondersteunen van de vertaling tussen de twee. Er zijn STIX-slider converts van STIX 2.x naar STIX 1.0 en STIX-elevator converts van STIX 1.0 naar STIX 2.x.

2.1.2. Betrokken experts evaluatie STIX

De volgende experts zijn betrokken geweest bij het onderzoek:

Voornaam	Achternaam	Organisatie
Luuk	Matthijssen	NCSC
Cees	Vaes	SSC-ICT
Chris	De Roode	SSC-ICT
Karl	Lovink	Belastingdienst
Pieter-Bas	Nederkoorn	VNG
Jan	Van Zessen	VNG
Twan	Van der Meer	IBD
Aukjan	Van Belkum	EclecticIQ
Melvin	Koelewijn	SURF
Ron	Spuijbroek	Agentschap Telecom (RDI)
Lars	Noordijk	Agentschap Telecom (RDI)

Tabel 1 - Betrokken experts evaluatie STIX

2.2. Evaluatie van STIX

Uit interviews kwam naar voren dat, zover bekend, vanuit de Nederlandse overheid niet of nauwelijks regie wordt gevoerd op de STIX standaard. Dit is opvallend aangezien cyberincidenten, zoals ransomware-aanvallen, aan de orde van de dag zijn. Cybersecurity wordt in belangrijke mate vanuit het perspectief van de dreiging en dus in termen van risico's wordt beleefd, aldus de Nederlandse Cybersecuritystrategie 2022-2028. In dit perspectief is het te verwachten dat de Nederlandse overheid een sturende rol, een regierol, wil hebben op de STIX standaard. Deze regierol draagt bij aan het vergroten van de digitale weerbaarheid door grip te houden op het beheerproces en op

de adoptie en zorgt ervoor dat Nederland aansluit bij internationale ontwikkelingen rond STIX en het melden van dreigingsinformatie.

Het NCSC heeft STIX 1.2.1. in 2017 aangemeld voor op de lijst met open standaarden – de 'pas toe of leg uit'-lijst,. Het NCSC geeft, tijdens het interview, aan geen contact te hebben met OASIS, de beheerorganisatie van de standaard. De medewerkers van het NCSC destijds betrokken bij de aanmelding van STIX zijn niet meer of elders werkzaam bij het NCSC. Het NCSC zit niet aan tafel bij OASIS en speelt internationaal geen rol in de ontwikkeling van nieuwe versies van de standaard. Daarnaast is er op dit moment geen inspanning bij het NCSC om de nieuwe versies van de standaard aan te melden, al wordt het belang er wel van ingezien.

Uit de interviews komt naar voren dat STIX een belangrijke rol heeft in betere informatie-uitwisseling van cyberdreigingsinformatie, en daarmee een betere digitale weerbaarheid. Tegelijkertijd is er geen andere overheidspartij naar voren gekomen die regie voert op de STIX standaard en de aansluiting op internationale ontwikkelingen. Deze bevinding biedt context voor enkele van de bevindingen uit dit rapport die hieronder volgen.

2.2.1. Toepassingsgebied

STIX kent het volgende functioneel toepassingsgebied:

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

Alle bevraagde experts ondersteunen het gedefinieerde toepassingsgebied. Het toepassingsgebied is concreet en helder geformuleerd.

Wel werd er genoemd dat het niet alleen digitale dreigingen tegen informatiesystemen betreft maar digitale dreigingen in het algemeen. Door het toepassingsgebied te specificeren op informatiesystemen is de scope iets te nauw, al is het niet onjuist.

2.2.2. Toegevoegde waarde

Toegevoegde waarde STIX niet ter discussie

Alle bevraagde experts zijn het er unaniem over eens dat de standaard STIX een duidelijke meerwaarde heeft.

De experts geven aan dat het onderwerp cyberdreiging/cybersecurity en de markt rondom cyberdreigingsinformatie steeds groter wordt. Het is een belangrijke ontwikkeling die steeds meer impact heeft in de wereld. Er ontstaat een hele industrie die zich bezig houdt met cybersecurity en die snel groeit. Meer en meer organisaties worden met dreigingen of zelfs aanvallen geconfronteerd. De Nederlandse Cybersecuritystrategie van 2022-2028 schetst hetzelfde beeld: "De digitale dreiging is permanent en neemt eerder toe dan af, met alle mogelijke gevolgen van dien.". Een van de geïdentificeerde uitdagingen met betrekking tot de digitale weerbaarheid is dat de afgelopen jaren is gebleken dat informatie-uitwisseling gefragmenteerd is, waardoor dreigingsinformatie niet altijd alle organisaties tijdig heeft bereikt en in staat heeft gesteld om maatregelen te treffen. De Baseline Informatiebeveiliging Overheid (BIO) beschrijft het basisniveau voor informatiebeveiliging. De BIO wordt gehanteerd binnen de Nederlandse overheid, door het Rijk, Gemeenten, Waterschappen en Provincies. Wijzigingen aan de BIO kunnen noodzakelijk zijn bijvoorbeeld bij nieuwe dreigingen, aldus de BIO versie 1. Een goed werkende en snelle informatie-uitwisseling is in deze situatie cruciaal. De STIX standaard helpt hierbij.

Bovendien is het van belang om onduidelijkheden op het moment van een dreiging te voorkomen, STIX helpt hierin door te definiëren wat er gecommuniceerd kan worden op een manier dat een persoon en een machine het kan begrijpen. Als je elkaar niet begrijpt dan kan dit zorgen voor vertraging, terwijl tijd van essentieel belang is in dergelijke situaties. Het hebben van een gedeelde taal (vocabulaire) helpt, ook op menselijk vlak. De termen worden eigen gemaakt en opgenomen in processen en modellen, zo kan men goed duiden waar het over gaat en dat komt uiteindelijk ten goede aan de snelheid van reageren. STIX voorkomt zodoende discussie over de termen die worden gebruikt bij het communiceren over dreigingen.

Agentschap Telecom geeft aan dat STIX en TAXII een belangrijke rol spelen in Vulnerability management en specifiek in het weerbaar zijn tegen ‘net bekende aanvallen’ en ‘onbekende aanvallen’. ‘Net bekende aanvallen’ moeten zo snel mogelijk op de juiste manier (format) bij organisaties bekend worden, om ze geautomatiseerd te kunnen verwerken en om zo snel mogelijk te reageren. ‘Onbekende aanvallen’ zijn de cyberaanvallen waar nog geen oplossing (ook wel bekend als patch) voor is. Voor deze zero-day kwetsbaarheden heeft de ontwikkelaar nog geen tijd gehad om een patch te ontwikkelen. Juist in de ‘onbekende aanvallen’ zit een levendige handel. Er is een hele markt aan partijen die erop gebrand zijn om nieuwe manieren te vinden om kwetsbaarheden te exploiteren. Snel reageren en handelen op een ‘onbekende aanval’ is essentieel. Informatieuitwisseling over deze aanvallen is van groot belang, en juist STIX en TAXII voorzien hierin.

Minimale impact op processen en systemen overheidsorganisaties

In basis zijn er geen aanpassingen nodig aan de processen of systemen van de (overheids)organisaties omdat STIX onderdeel is van aangeschafte cybersecuritysoftware. Wel bepaalt de standaard welke objecten en daarmee welke informatie er doorgegeven kan worden; de standaard beheerst de manier van informatie-uitwisseling. Een medewerker kan niet allerlei eigen informatie toevoegen, dit zou de werking van de standaard beïnvloeden. Met STIX 2.0/2.1 kan er specifiekere en daarmee rijkere informatie over dreigingen worden doorgegeven. De werkwijze zal daarmee iets veranderen, leveranciers stellen bij dit soort wijzigingen hun klanten (waaronder overheidsorganisaties) op de hoogte en adviseren over hoe de standaard het beste gebruikt kan worden.

Daarnaast geldt dat de ene leverancier het werken met de standaard gemakkelijker maakt dan de ander, dit is afhankelijk van de aangeboden software.

Potentiële waarde STIX en TAXII niet volledig benut

STIX en TAXII maken meer mogelijk dan alleen snelle informatie-uitwisseling. Doordat er een standaard format gehanteerd wordt is het mogelijk om vervolgacties te automatiseren, aldus Agentschap Telecom. Het binnenkomen van een ‘net bekende aanval’ of zero-day melding kan een aanleiding zijn om geautomatiseerd hiermee aan de gang te gaan, zodat het functioneert als een automatische trigger. Deze trigger kan het start zijn voor een geautomatiseerde analyse van het asset management, geautomatiseerd testen van oplossingen, en het geautomatiseerd deployen van een patch. Hiermee wordt veel tijd bespaard en kan er snel gereageerd worden op aanvallen.

Aanvullende middelen ondersteunen de standaard

Naast de specificaties van de standaarden is er een werkgroep, CTI STIX Subcommittee, die invulling geeft aan de standaard. Zo zijn er handreikingen en handleidingen hoe de standaard toegepast kan worden. Alleen een standaard is niet voldoende, er moeten tevens checklists, testen en andere hulpmiddelen worden ingezet om de werking te toetsen. Deze middelen, zoals handreikingen en checklists, zijn echter gericht op de leveranciers die STIX opnemen als een standaard is gebruikt in hun software.

Overheidsorganisaties geven aan zelf geen documentatie zoals handreikingen of handleidingen te gebruiken. Dit omdat de software die zij gebruiken al zijn verrijkt met de STIX standaard door de leverancier. Door overheidsorganisaties wordt er niet actief gecommuniceerd over hun ervaringen met het gebruik van de standaarden.

Toegevoegde waarde nieuwe versie: STIX 2.1

De nieuwe versie van de standaard is beter bruikbaar in processen. De nieuwe versie is meer gedetailleerd en het is daardoor gemakkelijker om te interpreteren waar de data over gaat. Er kan namelijk specifiekere dreigingsinformatie uitgewisseld worden.

Tegelijkertijd is dit een valkuil aangezien de standaard complexer is, iets wat de adoptie van de standaard in de weg kan staan. Agentschap Telecom geeft aan dat de complexiteit met name zit in de hoeveelheid aan cyberdreigingsinformatie wat met STIX en TAXII uitgewisseld kan worden. Het komen tot inzichten uit een grote hoeveelheid aan ruwe informatie is uitdagend, hier zijn data analisten voor nodig. Zij kunnen met hun technische kennis dreigingsbeelden creëren van de ruwe informatie. Dit maakt het mogelijk om daadwerkelijk digitaal weerbaar te zijn en om vanuit strategisch, tactisch en operationeel niveau te werken aan het vinden van oplossingen.

2.2.3. Draagvlak

Er is (nog) geen objectieve meetmethode om het gebruik van STIX inzichtelijk te maken. Het is wel zichtbaar dat nieuwe cybersecurity producten, zoals uitwisselingsdiensten van cybersecurity-informatie en geïntegreerde “security orchestration, automation and response-platformen” (SOAR-tooling) steeds vaker op de STIX en TAXII standaarden aansluiten, aldus de Monitor Open Standaarden 2021.

Adoptie op rijksniveau

Het Nationaal Cyber Security Center (NCSC) heeft als taak om Nederland weerbaar te maken tegen cyberdreigingen. Het NCSC maakt voor zijn dienstverlening onder meer gebruik van het Nationaal Detectie Netwerk (NDN) dat zich richt op het onderling delen van dreigings- en incidentinformatie.

Een van de producten van het Nationaal Detectie Netwerk (NDN) is het Threat Intel Platform (TIP). Voor TIP werken Rijksoverheidsorganisaties samen op het gebied van cyberdreigingen. In dit platform delen zij acute en relevante dreigingsinformatie en werken ze samen aan het analyseren van deze dreigingen. Dit is mogelijk door de samenwerkingsruimten die het Threat Intel platform biedt. Met het TIP kunnen dreigingen sneller opgezocht, gerelateerd en visueel zichtbaar gemaakt worden. Binnen het NDN creëert het NCSC, op basis van verkregen informatie, een breed en gemeenschappelijk beeld van de actuele cyberdreigingen. Het NCSC, de AIVD en de MIVD verzamelen informatie over cyberdreigingen en stellen die informatie beschikbaar aan het NDN. Organisaties die deelnemen aan het NDN leveren ook (anoniem) informatie volgens het Nationaal Detectie Netwerk infosheet. Het NCSC gebruikt de STIX standaard, informatie-uitwisseling op het platform gebeurt via de STIX en TAXII standaarden. Als overheidsorganisaties op het platform willen aansluiten dan moeten ze voldoen aan de standaarden, hiermee heeft het NCSC een disciplinerende functie.

Veel Rijksoverheidsorganisaties maken voor hun informatievoorziening en hun informatiebeveiliging gebruik van shared service organisaties (zoals SSC-ICT, DICTU, DUO, JIO, en SSC Campus). Deze shared service organisaties hebben SOC-afdelingen (Security Operations Center) waar de monitoring, detectie en afhandeling van informatiebeveiligingsincidenten is belegd. Het zijn vooral deze SOC’s die gebruikers zijn van de securitysystemen/platformen waar de STIX en TAXII standaarden op van toepassing zijn.

Binnen de Rijksoverheid zijn 155 van de 190 organisaties aangesloten bij het NDN waarvan 101 organisaties zijn aangesloten via de sensor van een shared service organisatie. Dat geeft een dekkingsgraad geeft van 82%, aldus de Monitor Open Standaarden 2021. Het aantal aangesloten partijen is in vergelijking met eerdere jaren toegenomen. Dit is een indicator van de trend dat binnen de Rijksoverheid het gebruik van securitysystemen/platformen voor de bescherming tegen cyberdreigingen langzaam maar zeker toeneemt.

Adoptie binnen de gemeenten

Voor veel gemeenten is er geen gestandaardiseerde manier beschikbaar om cyberdreigingsinformatie uit te wisselen, de redenen hiervoor worden hieronder toegelicht.

De Informatiebeveiligingsdienst (IBD) van Vereniging Nederlandse Gemeenten (VNG) faciliteert de uitwisseling van threat intelligence voor verschillende gemeenten, inclusief de deelnemers van de collectieve aanbesteding GGI-Veilig. Het grootste deel van de gemeenten heeft niet de kennis en capaciteit om eigenstandig het proces van threat intelligence uit te voeren. De adoptie van STIX zou in de gemeenten gerealiseerd worden doordat STIX werd opgenomen in de Gemeentelijke Gemeenschappelijke Infrastructuur (GGI). Hiervan was sprake totdat KPN, de VNG en de deelnemende gemeenten het contract voor het leveren van SIEM/SOC-diensten in goed overleg hebben beëindigd. Met dit contract zou KPN SIEM (security information and event management) en SOC (security operations center)-diensten leveren aan 211 deelnemers van de aanbesteding. In de aanbesteding van GGI-veilig zijn eisen aan de SIEM/SOC-diensten gesteld. Hierin staat onder andere dat de dreigingsinformatie bi-directioneel via een koppeling wordt gedeeld. Voor de uitwisseling van dreigingsinformatie geldt dat dit dient te gebeuren middels open standaarden (STIX/TAXII). Een verdere eis in de aanbesteding was dat de Advanced Threat Protection-oplossing het TAXII-protocol ondersteunt voor geautomatiseerde uitwisseling van cyberdreigingsinformatie (IoC's) op basis van het STIX-formaat.

Het opzeggen van het contract heeft gevolgen voor de gemeenten, de aanbesteding was voor bijna 90% van de gemeenten van toepassing. Gemeenten dienen de betreffende dienstverlening nu op andere wijze te verwerven. Er wordt nog nagedacht over een nieuwe collectieve verwerving of begeleiding bij verwerving.

De IBD geeft aan dat gemeenten steeds meer vragen naar het delen van dreigingsinformatie. De snelheid van de standaarden implementeren loopt helaas achter. Gemeenten hebben beperkte middelen om SIEM/SOC-diensten af te nemen. Wel willen ze graag aansluiten middels standaarden om dreigingsinformatie binnen te halen, aan de interesse ligt het niet. Er zijn wel enkele gemeenten die zijn aangesloten op het KPN-platform, in het kader van de eerste toetreders tot GGI-Veilig. Deze gemeenten zijn nog steeds operationeel maar moeten uiteindelijk over naar de MISP van de IBD.

Slechts enkele gemeenten halen op eigen initiatief dreigingsinformatie middels de STIX en TAXII standaarden binnen. Van deze gemeenten komen geen bijzondere signalen bij de IBD, de standaarden lijken te doen wat ze moeten doen.

De IBD heeft het Malware Information Sharing Platform (MISP) in gebruik genomen. Hierop zullen naar verwachting het komende jaar meer gemeenten en gemeentelijke leveranciers aangesloten worden, met een positief effect op de adoptie van STIX/TAXII.

Adoptie waterschappen en provincies

Vanuit het Computer Emergency Response Team – Watermanagement, kortweg CERT-WM, wordt er geen threat intelligence (TI) op een geautomatiseerde wijze uitgewisseld met de achterban, daarmee worden de STIX en TAXII standaarden niet gebruikt. In

CERT-WM werken de 21 waterschappen en Rijkswaterstaat samen aan informatiebeveiliging in de waterketen. Mocht hier verandering in komen dan ligt het gebruik van MISP voor de hand, en wordt daarmee mogelijk gebruik gemaakt van de standaarden.

Tijdens deze evaluatie is het niet gelukt om informatie over provincies op te halen.

Adoptie semioverheid

SURF geeft aan op dit moment geen gebruik te maken van de STIX en TAXII standaarden. Het Malware Information Sharing Platform (MISP) wordt gebruikt om informatie over cyberdreigingen uit te wisselen middels andere formaten en protocollen. Dit neemt niet weg dat het voor SURF in de toekomst wellicht wel relevant of nodig is om de STIX en TAXII standaarden te gaan gebruiken. Deze overstap zal gemaakt kunnen worden aangezien de systemen die SURF gebruikt, waaronder MISP, wel de standaarden ondersteunen.

STIX heeft draagvlak in het buitenland

Het gebruik van de STIX en TAXII standaarden wordt tevens benoemd in het richtsnoer voor het uitwisselen van cyberdreigingsinformatie van de Britse overheid bijgewerkt op 9 augustus 2022. In dit richtsnoer worden STIX 2 en TAXII 2 verplicht gesteld bij het gebruik van een cyberdreigingsinformatiesysteem.

Het Cyber Information Sharing and Collaboration Program (CISCP) van het Amerikaanse Department of Homeland Security (DHS) maakt bruikbare, relevante en tijdige informatie-uitwisseling mogelijk in alle sectoren met een kritieke infrastructuur. De verspreiding van cybersecurity informatie gebeurt door gebruik van STIX en TAXII, beschreven door de Cybersecurity & Infrastructure Security Agency (CISA). Bovendien wordt de STIX standaard gebruikt in de Automated Indicator Sharing (AIS) capability van de CISA, wat deelnemers aan de AIS community in staat stelt om real-time cyberdreigingsindicatoren en defensieve maatregelen uit te wisselen.

Marktondersteuning voor de standaard

STIX en TAXII zijn gebruikelijke standaarden in de markt. Het NSCS geeft aan dat de standaard STIX wordt gebruikt door softwarebedrijven die securitysystemen/platformen, zoals een Threat Intelligence Platform (TIP), ontwikkelen waarin cyberdreigingsinformatie wordt uitgewisseld. De klanten van deze softwarebedrijven zijn onder andere overheidsorganisaties.

VNG geeft aan dat in de aanbesteding voor GGI-Veilig er van 30 marktpartijen geen signaal kwam dat het conformeren aan de standaarden een uitdaging of drempel zou zijn.

Een analyse van de markt laat zien dat onder andere de volgende leveranciers van securitysystemen/platformen STIX en TAXII ondersteunen:

- Splunk
- HP ArcSight
- IBM QRadar
- Alienvault
- Anomali
- EclecticIQ
- ThreatQuotient
- ThreatConnect
- MISP (open source)

Het gedragen beeld van de experts is dat er voldoende keuze is aan leveranciers die de standaard gebruiken in hun softwarepakket. EclecticIQ geeft tijdens het interview aan dat STIX een van de standaarden is in hun software waarmee overheidsorganisaties inzicht krijgen in dreigingen. Voor deze evaluatie is er alleen gesproken met EclecticIQ.

Adoptie nieuwe versie: STIX 2.1

De adoptie van de nieuwe versie van STIX is afhankelijk van de leverancier en of deze leverancier de nieuwe versie van de standaard heeft opgenomen in zijn/haar software. EclecticIQ geeft aan de nieuwe versie te ondersteunen en deze ondersteuning ook bij veel andere leveranciers te zien. De Belastingdienst geeft aan dat hun leverancier nog niet over is op de nieuwe versie. De bevraagde experts denken dat leveranciers uiteindelijk wel over zullen gaan, anders prijzen ze zich uit de markt.

Het NCSC geeft aan dat STIX 1.x beperkt was in de hoeveelheid informatie dat ermee uitgewisseld kon worden. Leveranciers maakten eigen aanpassingen, maar op dat moment is het geen standaard meer doordat er varianten op de standaard ontstaan. Dit belemmert de uitwisseling. Ten opzichte van de oude versie 1.2.1 is een meer uitgebreide versie 2.0 vastgesteld die in de praktijk echter lastig bruikbaar is gebleken. Inmiddels zijn de kinderziektes verholpen en is een nieuwe versie 2.1 vastgesteld, die volgens NCSC veel beter bruikbaar is. Deze ervaringen belemmeren de adoptie en zorgen ervoor dat niet alle leveranciers zijn over gegaan. Op dit moment wordt de oude versie (1.x) nog meer gebruikt dan de nieuwe versie (2.1).

Het NCSC kan beide versies gebruiken. Het is van belang om aan te sluiten bij wat er door de gebruikers gehanteerd wordt. Het heeft geen nut als het NCSC slechts de nieuwe versie gebruikt terwijl gebruikers nog op de oude versie zitten. Dit staat dan de informatie-uitwisseling in de weg. Wel heeft het NCSC de voorkeur voor de nieuwste versie van de standaard, ook al wordt de oude versies voorlopig ondersteunt.

STIX en TAXII worden lang niet altijd (juist) gebruikt

Een kanttekening vanuit het NCSC is dat het maar ten dele waar is dat de meeste securitysystemen/platformen STIX ondersteunen. TIP systemen voor interne gegevensverwerking hanteren doorgaans een eigen opslagformaat. De ondersteuning van STIX bestaat dan uit de mogelijkheid om gegevens via een conversiemodule in STIX formaat te kunnen importeren en exporteren. Bij de aanschaf van software moet worden opgelet dat de standaard zodanig wordt toegepast dat de gegevens zo veel mogelijk verliesloos kunnen worden uitgewisseld met systemen van andere leveranciers.

Agentschap Telecom benadrukt dat weinig partijen, die werken in de operationele security en optimale weerbaarheid van systemen, STIX en TAXII juist gebruiken. Hierdoor wordt veel tijd verspilt aan analyses, onderzoek en het verspreiden van informatie en patches. Deels komt dit door de afhankelijkheid van de leverancier van securitysystemen/platformen en wat die aanbieden, deels door het niet bewust zijn van de mogelijkheden en waarde van STIX en TAXII.

2.2.4. Beheer

OASIS is een non-profit organisatie waarin mensen deelnemen om projecten voor cybersecurity, blockchain, IoT en meer verder te brengen. OASIS kent een Cyber Threat Intelligence (CTI) Technical Committee. Het doel van de commissie is het definiëren van oplossingen om cyberdreigingsinformatie te modelleren, analyseren en delen. De inspanningen zijn gebouwd op de werkzaamheden van de commissie aan de STIX en TAXII specificaties. Zo is er een STIX subcommittee en TAXII subcommittee. Documenten met betrekking tot vergaderingen van deze commissies zijn openbaar en te vinden op OASIS Open. Deelnemers aan deze commissies bestaan met name uit

medewerkers van (grote) marktpartijen: Accenture, Cisco Systems, EclecticIQ, IBM, NIST, en meer is te vinden op de lijst met members.

Geen enkele van de bevraagde experts van de overheidsorganisaties is betrokken bij het beheer of de verdere ontwikkeling van de standaard.

EclecticIQ geeft aan wel betrokken te zijn bij de beheerorganisatie. EclecticIQ is een sponsor van OASIS en neemt actief deel.

De ontwikkeling van een nieuwe versie van de standaard heeft plaats gevonden in samenwerking met veel leveranciers, daarmee is het een lang proces. Dit is deels te wijten aan het feit dat deelname vrijwillig is en daarmee vaak een extra activiteit voor de betrokkenen. EclecticIQ geeft aan dat het besluitvormingsproces prettig verloopt en dat het gehele proces zeer gedegen is opgezet door OASIS. Informatie over het besluitvormingsproces is niet openbaar beschikbaar.

2.2.5. Opname op de lijst

Op de vraag of opname op de lijst de adoptie van de STIX standaard heeft verhoogd wordt er meermaals ontkennend gereageerd. Het merendeel van de experts geeft aan dat de hoge mate van adoptie te danken is aan het feit dat een relatief kleine groep aan leveranciers de standaard hebben omarmd en opgenomen in hun software. De leveranciers zijn de drijvende kracht achter de adoptie van de STIX standaard. De Nederlandse overheid heeft in dit geval een beperkte rol in de adoptie van de standaard. Wel valt de groep aan leveranciers te beïnvloeden om een standaard te overwegen door een sterk signaal, waaronder de opname van de standaard op de ‘pas toe of leg uit’-lijst.

Het merendeel van de experts aan het prettig te vinden om de standaard op de ‘pas toe of leg uit’-lijst te hebben staan. Dit geeft een legitimiteit om de standaard verplicht te stellen via ‘pas toe of leg uit’-verplichting richting leverancier en het uit te vragen tijdens aanbestedingen. Deze onderhandelingspositie raken de experts liever niet kwijt. De standaard heeft betrekking op een zeer specifiek vakgebied waarin het prettig is om leveranciersonafhankelijk te kunnen zijn. In deze dynamiek heeft het waarde dat de standaard op de ‘pas toe of leg uit’-lijst staat.

Ook EclecticIQ vindt de opname van de standaard op de lijst prettig omdat er dan voor wordt gezorgd dat ook de publieke sector dezelfde taal spreekt, wat de samenwerking en interoperabiliteit ten goede komt.

Alle bevraagde experts geven aan dat de nieuwe versie van de standaard op de ‘pas toe of leg uit’-lijst moet komen te staan. De versie 1.x raakt inmiddels verouderd en het toepassen van deze standaarden zou tot problemen kunnen leiden. Bovendien helpt het wellicht om de leveranciers die nog niet over zijn te motiveren om de nieuwe versie te adopteren.

2.2.6. Status adoptie adviezen

Hieronder volgt er per adoptieadvies een statusupdate.

	Advies	Status
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	Dit is volgens de experts niet gebeurd. Het ontbreken van regie bij de Nederlandse overheid op de standaard

	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.	zorgt ervoor dat geen partij, zover bekend, zich hiervoor inspant. Het advies lijkt nog van belang te zijn aangezien experts aangeven dat versie 2 van de STIX standaard nog steeds ruimte laat voor verschil in gebruik.
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.	Dit is volgens de experts niet gebeurd. Het ontbreken van regie bij de Nederlandse overheid op de standaard zorgt ervoor dat geen partij, zover bekend, zich hiervoor inspant. Experts tonen geen interesse of behoefte in kennisbijeenkomsten t.a.v. het gebruik van STIX en TAXII. Het bezitten en verspreiden van kennis over gebruik van de standaard wordt als verantwoordelijkheid van de leveranciers van securitysystemen/platformen gezien. Tegelijkertijd lijkt het advies nog steeds relevant doordat onder andere gemeenten en waterschappen niet of nauwelijks gebruik maken van de standaard. Bovendien wordt de standaard niet altijd (juist) gebruikt of weet men niet van het potentieel wat de standaard, naast informatie-uitwisseling, kan bieden.
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.	Dit is volgens de experts niet gebeurd. Het advies lijkt nog steeds relevant aangezien gemeenten en waterschappen niet of nauwelijks gebruik maken van de standaard. Bovendien wordt de standaard niet altijd (juist) gebruikt of weet men niet van het potentieel wat de standaard, naast informatie-uitwisseling, kan bieden.
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.	Dit is volgens de experts niet gebeurd. Wel wordt er uitleg gedeeld over dreigingsinformatie. Experts tonen geen interesse of behoefte in het delen van informatie over de meerwaarde en best practices. Tegelijkertijd lijkt het advies nog steeds relevant doordat onder andere gemeenten en waterschappen niet of nauwelijks gebruik maken van de standaard.

		Bovendien wordt de standaard niet altijd (juist) gebruikt of weet men niet van het potentieel wat de standaard, naast informatie-uitwisseling, kan bieden.
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).	Hier was sprake van maar staat nu stil doordat het betreffende contract is ontbonden. Het advies is nog steeds relevant doordat gemeenten en waterschappen op dit moment niet of nauwelijks gebruik maken van de standaarden.

Tabel 2 - Status adoptieadviezen

2.2.7. Lopende ontwikkelingen

De experts geven aan dat het onderwerp cyberdreiging/cybersecurity en de markt rondom cyberdreigingsinformatie steeds groter wordt. Het is een belangrijke ontwikkeling die steeds meer impact heeft in de wereld. Meer en meer organisaties worden met dreigingen of zelfs aanvallen geconfronteerd. De Nederlandse Cybersecuritystrategie 2022-2028 schetst hetzelfde beeld: “De digitale dreiging is permanent en neemt eerder toe dan af, met alle mogelijke gevolgen van dien.”. Een van de geïdentificeerde uitdagingen met betrekking tot de digitale weerbaarheid van de afgelopen jaren is dat informatie-uitwisseling gefragmenteerd is, waardoor dreigingsinformatie niet altijd alle organisaties tijdig bereikt en organisaties niet tijdig in staat worden gesteld om maatregelen te treffen.

Er zijn andere standaarden die in hetzelfde domein opereren, deze richten zich echter niet specifiek op dreigingsinformatie, zoals OCSF. Dit soort standaarden zijn complementair en zullen op korte termijn geen vervanging voor de STIX standaard betekenen. Er zijn ook andere tools, modellen of kennisproducten specifiek voor cyberdreigingsinformatie, zoals Diamond model en Mittre ATT&CK. Vooralsnog ziet het NCSC deze als complementair aan de STIX-standaard.

Cybersecurity is een vakgebied in ontwikkeling, er is veel beweging maar het is moeilijk om te voorspellen waar het heen gaat. Het is goed denkbaar dat er nieuwe ontwikkelingen komen die de standaard overbodig zullen maken, maar vooralsnog is hier geen sprake van.

2.3. Conclusies en aanbevelingen STIX

2.3.1. Conclusies STIX

De meest opvallende conclusie is het ontbreken van een regierol vanuit de Nederlandse overheid op de STIX standaard, voor zover deze evaluatie dit kon achterhalen (zie ook paragraaf 2.2 Evaluatie van STIX). Er is geen betrokkenheid vanuit de Nederlandse overheid bij de beheerorganisatie OASIS. Enkele van de bevindingen hieronder zijn het gevolg van het ontbreken van deze regierol.

Toepassingsgebied

Het toepassingsgebied is correct geformuleerd. Een enkele opmerking over een aanscherping geeft geen aanleiding om de formulering van het toepassingsgebied te herzien.

Toegevoegde waarde

De toegevoegde waarde van de STIX-standaard staat niet ter discussie. Voor de overheidspartijen lijkt het vanzelfsprekend te zijn dat er in een situatie met toenemende cyberdreigingen een standaard is die de uitwisseling van cyberdreigingsinformatie faciliteert. De werking van de standaard staat in de basis niet ter discussie, wel zijn er ervaringen die opgepakt worden door de STIX subcommittee ter verbetering van de standaard.

Het potentieel van de STIX standaard om te komen tot snelle en geautomatiseerde reacties op aanvallen is niet altijd bekend bij overheidspartijen.

Draagvlak

De adoptie van de standaard op rijksniveau is hoog. De meeste experts schrijven het succes toe aan de leveranciers die de standaard implementeren in hun producten. Het draagvlak van de standaard op rijksniveau is groot, ook de adoptie door de markt is groot. Een kanttekening is het lage adoptieniveau door gemeenten en waterschappen.

Overheidspartijen zijn afhankelijk van de leveranciers in de werking van de standaard en in welke versie van de standaard wordt gebruikt. Experts geven aan dat de adoptie van de nieuwe versie achterblijft, mede doordat leveranciers nog niet allemaal over zijn op de nieuwe versie.

Het NCSC gebruikt beide versies van de standaard. Dit geeft geen signaal of motivatie aan anderen om de nieuwe versie van de standaard te adopteren, waardoor de adoptie van de nieuwe versie niet bevorderd wordt.

Beheer

De standaard wordt actief beheerd door OASIS. Daarentegen is er geen regierol vanuit de Nederlandse overheid op de STIX standaard. De aanmelder van de standaard, NCSC, heeft niet of nauwelijks contact met de beheersorganisatie. Er is geen aansluiting bij OASIS vanuit de Nederlandse overheid.

Opname op de ‘pas toe of leg uit’-lijst

Alle bevraagde experts beamen dat de standaard, en met name de nieuwe versie STIX 2.1, opgenomen moet worden op de ‘pas toe of leg uit’-lijst. Dit biedt overheidspartijen een formele grondslag en extra motivatie om de nieuwe versie van de standaard uit te vragen. Tegelijkertijd schrijven de bevraagde experts de hoge adoptiegraad toe aan de leveranciers van securitysystemen/platformen die de standaard in hun systemen implementeren. Deze leveranciers zijn de drijvende kracht in de adoptie van de standaard, maar kunnen wel beïnvloed worden door een sterk signaal vanuit de Nederlandse overheid zoals de opname op de ‘pas toe of leg uit’-lijst.

Status adoptieadviezen

De adoptieadviezen zijn niet of nauwelijks opgevolgd. De regie mist op deze standaard hetgeen eraan bijdraagt dat opvolging van adoptieadviezen nergens landt. De bevraagde experts geven geen signalen dat er behoefte is aan kennisdeling, workshop of best practices. Tegelijkertijd is te zien dat de adoptie in sectoren achter blijft, zoals bij gemeenten en waterschappen, waardoor de gestelde adoptieadviezen nog steeds relevantie hebben.

Lopende ontwikkelingen

De lopende ontwikkelingen tonen dat cyberdreigingen steeds relevanter worden en dat de markt hieromheen toeneemt. De standaarden spelen hier een belangrijke rol in. Vooralsnog worden er geen ontwikkelingen voorzien die dit zouden veranderen.

2.3.2. Aanbevelingen STIX

Vanuit de analyse van de interviews en de bovenstaande conclusies zijn de volgende aanbevelingen opgesteld aan het Forum standaardisatie:

1. In gesprek gaan met het NCSC over de regierol op de STIX standaard gezien het NCSC de aanmelder van de STIX standaard op de ‘pas toe of leg uit’-lijst is geweest.

2. In samenwerking met het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties afdeling Digitale Samenleving onderzoeken waar de regierol voor de STIX standaard binnen de Nederlandse overheid het beste is belegd en hierover adviseren.

3. De markt rondom cyberdreigingsinformatie groeit en is in beweging. De kans dat er op een middellange termijn ontwikkelingen zijn die de standaarden raken is groot. Het advies is om tussen de twee en vier jaar de standaard opnieuw te evalueren.

Zodra de regierol voor de STIX standaard belegd is binnen de Nederlandse overheid dan zijn de volgende aanbevelingen aan de partij die de regierol op zich neemt gericht:

4. Contact leggen met partijen die actief zijn in de STIX committee bij de beheerorganisatie OASIS met als doel om zicht en grip te krijgen op het beheerproces en op internationale ontwikkelingen.

5. Opnieuw onderzoeken van het nut en de noodzaak van de adoptieadviezen. De experts geven geen signalen dat er behoefte is aan kennisdeling over de standaard. Daarentegen loopt de adoptie bij gemeenten en waterschappen achter en is de potentiële meerwaarde van de standaard niet helder voor alle organisaties.

6. Uitdragen en communiceren van toegevoegde waarde van de STIX standaard.

7. Onderzoek in hoeverre er sprake is van leveranciersafhankelijkheid bij de STIX standaard door de sterke rol van leveranciers in de ontwikkeling en het uitdragen van de standaard.

3. Evaluatie TAXII

3.1. Inleiding

3.1.1. Toelichting TAXII standaard

Trusted Automated eXchange of Indicator Information (TAXII™) draagt bij aan het geautomatiseerd en in real-time uitwisselen van cyberdreigingsinformatie doordat het een toepassingsprotocol biedt 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, en het stelt organisaties in staat om de informatie gemakkelijk te delen met partners.

TAXII is speciaal ontworpen om de uitwisseling van cyberdreigingsinformatie die in STIX wordt vertegenwoordigd te ondersteunen. 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.

Verschil TAXII 1.x en TAXII 2.x

Op de ‘pas toe of leg uit’-lijst is TAXII 1.1.1 opgenomen. Inmiddels is TAXII 2.1 uitgebracht.

TAXII 2.1 definieert inmiddels twee diensten die, indien geïmplementeerd, het delen van bruikbare informatie over cyberdreigingen mogelijk maken over organisatie- en product-/servicegrenzen heen. TAXII definieert een RESTful API (een set services en berichtenuitwisselingen) en een set vereisten voor TAXII-clients en -servers. De verschillen tussen TAXII 1.x en 2.x zijn klein.

3.1.2. Betrokken experts evaluatie TAXII

De volgende experts zijn betrokken geweest bij het onderzoek:

Voornaam	Achternaam	Organisatie
Luuk	Matthijssen	NCSC
Cees	Vaes	SSC-ICT
Chris	De Roode	SSC-ICT
Karl	Lovink	Belastingdienst
Pieter-Bas	Nederkoorn	VNG
Jan	Van Zessen	VNG
Twan	Van der Meer	IBD

Aukjan	Van Belkum	EclecticIQ
Melvin	Koelewijn	SURF
Ron	Spuijbroek	Agentschap Telecom (RDI)
Lars	Noordijk	Agentschap Telecom (RDI)

Tabel 3 - Betrokken experts evaluatie TAXII

3.2. Evaluatie van TAXII

Uit interviews kwam naar voren dat, zover bekend, vanuit de Nederlandse overheid niet of nauwelijks regie wordt gevoerd op de TAXII standaard. Dit is opvallend aangezien cyberincidenten, zoals ransomware-aanvallen, aan de orde van de dag zijn. Cybersecurity wordt in belangrijke mate vanuit het perspectief van de dreiging en dus in termen van risico's wordt beleefd, aldus de Nederlandse Cybersecuritystrategie 2022-2028. In dit perspectief is het te verwachten dat de Nederlandse overheid een sturende rol, een regierol, wil hebben op de TAXII standaard. Deze regierol draagt bij aan het vergroten van de digitale weerbaarheid door grip te houden op het beheerproces en op de adoptie en zorgt ervoor dat Nederland aansluit bij internationale ontwikkelingen rond TAXII en het melden van dreigingsinformatie.

Het NCSC heeft TAXII 1.1.1. in 2017 aangemeld voor op de lijst met open standaarden – de 'pas toe of leg uit'-lijst. Het NCSC geeft, tijdens het interview, aan geen contact te hebben met OASIS, de beheerorganisatie van de standaard. De medewerkers van het NCSC destijds betrokken bij de aanmelding van TAXII zijn niet meer of elders werkzaam bij het NCSC. Het NCSC zit niet aan tafel bij OASIS en speelt internationaal geen rol in de ontwikkeling van nieuwe versies van de standaard. Daarnaast is er op dit moment geen inspanning bij het NCSC om de nieuwe versies van de standaard aan te melden, al wordt het belang er wel van ingezien.

Uit de interviews komt naar voren dat TAXII een belangrijke rol heeft in betere informatie-uitwisseling van cyberdreigingsinformatie, en daarmee een betere digitale weerbaarheid. Tegelijkertijd is er geen andere overheidspartij naar voren gekomen die regie voert op de TAXII standaard en de aansluiting op internationale ontwikkelingen. Deze bevinding biedt context voor enkele van de bevindingen uit dit rapport die hieronder volgen.

3.2.1. Toepassingsgebied

TAXII kent het volgende functioneel toepassingsgebied:

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

Alle bevraagde experts ondersteunen het gedefinieerde toepassingsgebied. Het toepassingsgebied is concreet en helder geformuleerd.

Wel werd er genoemd dat het niet alleen digitale dreigingen tegen informatiesystemen betreft maar digitale dreigingen in het algemeen. Door het toepassingsgebied te specificeren op informatiesystemen is de scope iets te nauw, al is het niet onjuist.

3.2.2. Toegevoegde waarde

Toegevoegde waarde niet ter discussie

Alle bevraagde experts zijn het er unaniem over eens dat de standaard TAXII een duidelijke meerwaarde heeft.

De experts geven aan dat het onderwerp cyberdreiging/cybersecurity en de markt rondom cyberdreigingsinformatie steeds groter wordt. Het is een belangrijke ontwikkeling die steeds meer impact heeft in de wereld. Er ontstaat een hele industrie die zich bezig houdt met cybersecurity en die snel groeit. Meer en meer organisaties worden met dreigingen of zelfs aanvallen geconfronteerd. De Nederlandse Cybersecuritystrategie van 2022-2028 schetst hetzelfde beeld: “De digitale dreiging is permanent en neemt eerder toe dan af, met alle mogelijke gevolgen van dien.”. Een van de geïdentificeerde uitdagingen met betrekking tot de digitale weerbaarheid is dat de afgelopen jaren is gebleken dat informatie-uitwisseling gefragmenteerd is, waardoor dreigingsinformatie niet altijd alle organisaties tijdig heeft bereikt en in staat heeft gesteld om maatregelen te treffen. De Baseline Informatiebeveiliging Overheid (BIO) beschrijft het basisniveau voor informatiebeveiliging. De BIO wordt gehanteerd binnen de Nederlandse overheid, door het Rijk, Gemeenten, Waterschappen en Provincies. Wijzigingen aan de BIO kunnen noodzakelijk zijn bijvoorbeeld bij nieuwe dreigingen, aldus de BIO versie 1. Een goed werkende en snelle informatie-uitwisseling is in deze situatie cruciaal. De TAXII standaard helpt hierbij.

Dagelijks halen organisaties grote hoeveelheden aan data binnen over de TAXII protocollen. Dit is een continu proces.

Agentschap Telecom geeft aan dat STIX en TAXII een belangrijke rol spelen in Vulnerability management en specifiek in het weerbaar zijn tegen ‘net bekende aanvallen’ en ‘onbekende aanvallen’. ‘Net bekende aanvallen’ moeten zo snel mogelijk op de juiste manier (format) bij organisaties bekend worden, om ze geautomatiseerd te kunnen verwerken en om zo snel mogelijk te reageren. ‘Onbekende aanvallen’ zijn de cyberaanvallen waar nog geen oplossing (ook wel bekend als patch) voor is. Voor deze zero-day kwetsbaarheden heeft de ontwikkelaar nog geen tijd gehad om een patch te ontwikkelen. Juist in de ‘onbekende aanvallen’ zit een levendige handel. Er is een hele markt aan partijen die erop gebrand zijn om nieuwe manieren te vinden om kwetsbaarheden te exploiteren. Snel reageren en handelen op een ‘onbekende aanval’ is essentieel. Informatieuitwisseling over deze aanvallen is van groot belang, en juist STIX en TAXII voorzien hierin.

Minimale impact op processen en systemen overheidsorganisaties

In basis zijn er geen aanpassingen nodig aan de processen of systemen van de (overheids)organisaties om met de TAXII standaard te kunnen werken, omdat TAXII onderdeel is van aangeschafte software.

Potentiële waarde STIX en TAXII niet volledig benut

STIX en TAXII maken meer mogelijk dan alleen snelle informatie-uitwisseling. Doordat er een standaard format gehanteerd wordt is het mogelijk om vervolgacties te automatiseren, aldus Agentschap Telecom. Het binnenkomen van een ‘net bekende aanval’ of zero-day melding kan een aanleiding zijn om geautomatiseerd hiermee aan de gang te gaan, zodat het functioneert als een automatische trigger. Deze trigger kan het start zijn voor een geautomatiseerde analyse van het asset management, geautomatiseerd testen van oplossingen, en het geautomatiseerd deployen van een patch. Hiermee wordt veel tijd bespaard en kan er snel gereageerd worden op aanvallen.

Aanvullende middelen ondersteunen de standaard

Overheidsorganisaties geven aan zelf geen documentatie zoals handreikingen of handleidingen te gebruiken. Dit omdat de software die zij gebruiken al zijn verrijkt met de TAXII standaard door de leverancier. Door overheidsorganisaties wordt er niet actief gecommuniceerd over hun ervaringen met het gebruik van de standaarden.

3.2.3. Draagvlak

Er is (nog) geen objectieve meetmethode om het gebruik van TAXII inzichtelijk te maken. Het is wel zichtbaar dat nieuwe cybersecurity producten, zoals uitwisselingsdiensten van cybersecurity-informatie en geïntegreerde “security orchestration, automation and response-platformen” (SOAR-tooling) steeds vaker op de STIX en TAXII standaarden aansluiten, aldus de Monitor Open Standaarden 2021.

Adoptie op rijksniveau

Het Nationaal Cyber Security Center (NCSC) heeft als taak om Nederland weerbaar te maken tegen cyberdreigingen. Het NCSC maakt voor zijn dienstverlening onder meer gebruik van het Nationaal Detectie Netwerk (NDN) dat zich richt op het onderling delen van dreigings- en incidentinformatie.

Een van de producten van het Nationaal Detectie Netwerk (NDN) is het Threat Intel Platform (TIP). Voor TIP werken Rijksoverheidsorganisaties samen op het gebied van cyberdreigingen. In dit platform delen zij acute en relevante dreigingsinformatie en werken ze samen aan het analyseren van deze dreigingen. Dit is mogelijk door de samenwerkingsruimten die het Threat Intel platform biedt. Met het TIP kunnen dreigingen sneller opgezocht, gerelateerd en visueel zichtbaar gemaakt worden. Binnen het NDN creëert het NCSC, op basis van verkregen informatie, een breed en gemeenschappelijk beeld van de actuele cyberdreigingen. Het NCSC, de AIVD en de MIVD verzamelen informatie over cyberdreigingen en stellen die informatie beschikbaar aan het NDN. Organisaties die deelnemen aan het NDN leveren ook (anoniem) informatie volgens het Nationaal Detectie Netwerk infosheet. Het NCSC gebruikt de TAXII standaard, informatie-uitwisseling op het platform gebeurt via de STIX en TAXII standaarden. Als overheidsorganisaties op het platform willen aansluiten dan moeten ze voldoen aan de standaarden, hiermee heeft het NCSC een disciplinerende functie.

Veel Rijksoverheidsorganisaties maken voor hun informatievoorziening en hun informatiebeveiliging gebruik van shared service organisaties (zoals SSC-ICT, DICTU, DUO, JIO, en SSC Campus). Deze shared service organisaties hebben SOC-afdelingen (Security Operations Center) waar de monitoring, detectie en afhandeling van informatiebeveiligingsincidenten is belegd. Het zijn vooral deze SOC’s die gebruikers zijn van de securitysystemen/platformen waar de STIX en TAXII standaarden op van toepassing zijn.

Binnen de Rijksoverheid zijn 155 van de 190 organisaties aangesloten bij het NDN waarvan 101 organisaties zijn aangesloten via de sensor van een shared service organisatie. Dat geeft een dekkingsgraad geeft van 82%, aldus de Monitor Open Standaarden 2021. Het aantal aangesloten partijen is in vergelijking met eerdere jaren toegenomen. Dit is een indicator van de trend dat binnen de Rijksoverheid het gebruik van securitysystemen/platformen voor de bescherming tegen cyberdreigingen langzaam maar zeker toeneemt.

Adoptie binnen de gemeenten

Voor veel gemeenten is er geen gestandaardiseerde manier beschikbaar om cyberdreigingsinformatie uit te wisselen, de redenen hiervoor worden hieronder toegelicht.

De Informatiebeveiligingsdienst (IBD) van Vereniging Nederlandse Gemeenten (VNG) faciliteert de uitwisseling van threat intelligence voor verschillende gemeenten, inclusief de deelnemers van de collectieve aanbesteding GGI-Veilig. Het grootste deel van de gemeenten heeft niet de kennis en capaciteit om eigenstandig het proces van threat intelligence uit te voeren. De adoptie van TAXII zou in de gemeenten gerealiseerd worden doordat TAXII werd opgenomen in de Gemeentelijke Gemeenschappelijke

Infrastructuur (GGI). Hiervan was sprake totdat KPN, de VNG en de deelnemende gemeenten het contract voor het leveren van SIEM/SOC-diensten in goed overleg hebben beëindigd. Met dit contract zou KPN SIEM (security information and event management) en SOC (security operations center)-diensten leveren aan 211 deelnemers van de aanbesteding. In de aanbesteding van GGI-veilig zijn eisen aan de SIEM/SOC-diensten gesteld. Hierin staat onder andere dat de dreigingsinformatie bi-directioneel via een koppeling wordt gedeeld. Voor de uitwisseling van dreigingsinformatie geldt dat dit dient te gebeuren middels open standaarden (STIX/TAXII). Een verdere eis in de aanbesteding was dat de Advanced Threat Protection-oplossing het TAXII-protocol ondersteunt voor geautomatiseerde uitwisseling van cyberdreigingsinformatie (IoC's) op basis van het STIX-formaat.

Het opzeggen van het contract heeft gevolgen voor de gemeenten, de aanbesteding was voor bijna 90% van de gemeenten van toepassing. Gemeenten dienen de betreffende dienstverlening nu op andere wijze te verwerven. Er wordt nog nagedacht over een nieuwe collectieve verwerving of begeleiding bij verwerving.

De IBD geeft aan dat gemeenten steeds meer vragen naar het delen van dreigingsinformatie. De snelheid van de standaarden implementeren loopt helaas achter. Gemeenten hebben beperkte middelen om SIEM/SOC-diensten af te nemen. Wel willen ze graag aansluiten middels standaarden om dreigingsinformatie binnen te halen, aan de interesse ligt het niet. Er zijn wel enkele gemeenten die zijn aangesloten op het KPN-platform, in het kader van de eerste toetreders tot GGI-Veilig. Deze gemeenten zijn nog steeds operationeel maar moeten uiteindelijk over naar de MISP van de IBD.

Slechts enkele gemeenten halen op eigen initiatief dreigingsinformatie middels de STIX en TAXII standaarden binnen. Van deze gemeenten komen geen bijzondere signalen bij de IBD, de standaarden lijken te doen wat ze moeten doen.

De IBD heeft het Malware Information Sharing Platform (MISP) in gebruik genomen. Hierop zullen naar verwachting het komende jaar meer gemeenten en gemeentelijke leveranciers aangesloten worden, met een positief effect op de adoptie van STIX/TAXII.

Adoptie waterschappen en provincies

Vanuit het Computer Emergency Response Team – Watermanagement, kortweg CERT-WM, wordt er geen threat intelligence (TI) op een geautomatiseerde wijze uitgewisseld met de achterban, daarmee worden de STIX en TAXII standaarden niet gebruikt. In CERT-WM werken de 21 waterschappen en Rijkswaterstaat samen aan informatiebeveiliging in de waterketen. Mocht hier verandering in komen dan ligt het gebruik van MISP voor de hand, en wordt daarmee mogelijk gebruik gemaakt van de standaarden.

Tijdens deze evaluatie is het niet gelukt om informatie over provincies op te halen.

Adoptie semioverheid

SURF geeft aan op dit moment geen gebruik te maken van de STIX en TAXII standaarden. Het Malware Information Sharing Platform (MISP) wordt gebruikt om informatie over cyberdreigingen uit te wisselen middels andere formaten en protocollen. Dit neemt niet weg dat het voor SURF in de toekomst wellicht wel relevant of nodig is om de STIX en TAXII standaarden te gaan gebruiken. Deze overstap zal gemaakt kunnen worden aangezien de systemen die SURF gebruikt, waaronder MISP, wel de standaarden ondersteunen.

TAXII heeft draagvlak in het buitenland

Het gebruik van de STIX en TAXII standaarden wordt tevens benoemd in het richtsnoer voor het uitwisselen van cyberdreigingsinformatie van de Britse overheid bijgewerkt op 9 augustus 2022. In dit richtsnoer worden STIX 2 en TAXII 2 verplicht gesteld bij het gebruik van een cyberdreigingsinformatiesysteem.

Het Cyber Information Sharing and Collaboration Program (CISCP) van het Amerikaanse Department of Homeland Security (DHS) maakt bruikbare, relevante en tijdige informatie-uitwisseling mogelijk in alle sectoren met een kritieke infrastructuur. De verspreiding van cybersecurity informatie gebeurt door gebruik van STIX en TAXII, beschreven door de Cybersecurity & Infrastructure Security Agency (CISA). Bovendien wordt de TAXII standaard gebruikt in de Automated Indicator Sharing (AIS) capability van de CISA, wat deelnemers aan de AIS community in staat stelt om real-time cyberdreigingsindicatoren en defensieve maatregelen uit te wisselen.

Marktondersteuning voor de standaard

STIX en TAXII zijn gebruikelijke standaarden in de markt. Het NSCS geeft aan dat de TAXII standaard wordt gebruikt door softwarebedrijven die securitysystemen/platformen, zoals een Threat Intelligence Platform (TIP), ontwikkelen waarin cyberdreigingsinformatie wordt uitgewisseld. De klanten van deze softwarebedrijven zijn onder andere overheidsorganisaties. VNG geeft aan dat in de aanbesteding voor GGI-Veilig er van 30 marktpartijen geen signaal kwam dat het conformeren aan de standaarden een uitdaging of drempel zou zijn.

Een analyse van de markt laat zien dat onder andere de volgende leveranciers van securitysystemen/platformen STIX en TAXII ondersteunen:

- Splunk
- HP ArcSight
- IBM QRadar
- Alienvault
- Anomali
- EclecticIQ
- ThreatQuotient
- ThreatConnect
- MISP (open source)

Het gedragen beeld van de experts is dat er voldoende keuze is aan leveranciers die de standaard gebruiken in hun softwarepakket. EclecticIQ geeft tijdens het interview aan dat TAXII een van de standaarden is in hun software waarmee overheidsorganisaties inzicht krijgen in dreigingen. Voor deze evaluatie is er alleen gesproken met EclecticIQ.

Adoptie nieuwe versie: TAXII 2.x

De adoptie van de nieuwe versie van TAXII, namelijk 2.0 of 2.1 is afhankelijk van de leverancier en of deze leverancier de nieuwe versie van de standaard heeft opgenomen in zijn/haar software. EclecticIQ geeft aan de nieuwe versie te ondersteunen en deze ondersteuning ook bij veel andere leveranciers te zien. De Belastingdienst geeft aan dat hun leverancier nog niet over is op de nieuwe versie. De bevraagde experts denken dat leveranciers uiteindelijk wel over zullen gaan, anders prijzen ze zich uit de markt.

Het NCSC kan beide versies gebruiken. Het is van belang om aan te sluiten bij wat er door de gebruikers gehanteerd wordt. Het heeft geen nut als het NCSC slechts de nieuwe versie gebruikt terwijl gebruikers nog op de oude versie zitten. Dit staat dan de informatie-uitwisseling in de weg. Wel heeft het NCSC de voorkeur voor de nieuwste versie van de standaard, ook al wordt de oude versies voorlopig ondersteunt.

STIX en TAXII worden lang niet altijd (juist) gebruikt

Agentschap Telecom benadrukt dat weinig partijen, die werken in de operationele security en optimale weerbaarheid van systemen, STIX en TAXII juist gebruiken. Hierdoor wordt veel tijd verspilt aan analyses, onderzoek en het verspreiden van informatie en patches. Deels komt dit door de afhankelijkheid van de leverancier van securitysystemen/platformen en wat die aanbieden, deels door het niet bewust zijn van de mogelijkheden en waarde van STIX en TAXII.

3.2.4. Beheer

OASIS is een non-profit organisatie waarin mensen deelnemen om projecten voor cybersecurity, blockchain, IoT en meer verder te brengen. OASIS kent een Cyber Threat Intelligence (CTI) Technical Committee. Het doel van de commissie is het definiëren van oplossingen om cyberdreigingsinformatie te modelleren, analyseren en delen. De inspanningen zijn gebouwd op de werkzaamheden van de commissie aan de STIX en TAXII specificaties. Zo is er een STIX subcommittee en TAXII subcommittee. Documenten met betrekking tot vergaderingen van deze commissies zijn openbaar en te vinden op OASIS Open. Deelnemers aan deze commissies bestaan met name uit medewerkers van (grote) marktpartijen: Accenture, Cisco Systems, EclecticIQ, IBM, NIST, en meer is te vinden op de lijst met members.

Geen enkele van de bevraagde experts van de overheidsorganisaties is betrokken bij het beheer of de verdere ontwikkeling van de standaard.

EclecticIQ geeft aan wel betrokken te zijn bij de beheerorganisatie. EclecticIQ is een sponsor van OASIS en neemt actief deel.

De ontwikkeling van een nieuwe versie van de standaard heeft plaats gevonden in samenwerking met veel leveranciers, daarmee is het een lang proces. Dit is deels te wijten aan het feit dat deelname vrijwillig is en daarmee vaak een extra activiteit voor de betrokkenen. EclecticIQ geeft aan dat het besluitvormingsproces prettig verloopt en dat het gehele proces zeer gedegen is opgezet door OASIS. Informatie over het besluitvormingsproces is niet openbaar beschikbaar.

3.2.5. Opname op de lijst

Op de vraag of opname op de lijst de adoptie van de TAXII standaard heeft verhoogd wordt er meermaals ontkennend gereageerd. Het merendeel van de experts geeft aan dat de hoge mate van adoptie te danken is aan het feit dat een relatief kleine groep aan leveranciers de standaard hebben omarmd en opgenomen in hun software. De leveranciers zijn de drijvende kracht achter de adoptie van de TAXII standaard. De Nederlandse overheid heeft in dit geval een beperkte rol in de adoptie van de standaard. Wel valt de groep aan leveranciers te beïnvloeden om een standaard te overwegen door een sterk signaal, waaronder de opname van de standaard op de ‘pas toe of leg uit’-lijst.

Het merendeel van de experts aan het prettig te vinden om de standaard op de ‘pas toe of leg uit’-lijst te hebben staan. Dit geeft een legitimiteit om de standaard verplicht te stellen via ‘pas toe of leg uit’-verplichting richting leverancier en het uit te vragen tijdens aanbestedingen. Deze onderhandelingspositie raken de experts liever niet kwijt. De standaard heeft betrekking op een zeer specifiek vakgebied waarin het prettig is om leveranciersonafhankelijk te kunnen zijn. In deze dynamiek heeft het waarde dat de standaard op de ‘pas toe of leg uit’-lijst staat.

Ook EclecticIQ vindt de opname van de standaard op de lijst prettig omdat er dan voor wordt gezorgd dat ook de publieke sector dezelfde taal spreekt, wat de samenwerking en interoperabiliteit ten goede komt.

Alle bevraagde experts geven aan dat de nieuwe versie van de standaard op de ‘pas toe of leg uit’-lijst moet komen te staan. De versie 1.x raakt inmiddels verouderd en het toepassen van deze standaarden zou tot problemen kunnen leiden. Bovendien helpt het wellicht om de leveranciers die nog niet over zijn te motiveren om de nieuwe versie te adopteren.

3.2.6. Status adoptie adviezen

Hieronder volgt er per adoptieadvies een statusupdate.

	Advies	Status
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.	Dit is volgens de experts niet gebeurd. Het ontbreken van regie bij de Nederlandse overheid op de standaard zorgt ervoor dat geen partij, zover bekend, zich hiervoor inspant. Het advies lijkt specifiek voor STIX bedoeld te zijn.
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.	Dit is volgens de experts niet gebeurd. Het ontbreken van regie bij de Nederlandse overheid op de standaard zorgt ervoor dat geen partij, zover bekend, zich hiervoor inspant. Experts tonen geen interesse of behoefte in kennisbijeenkomsten t.a.v. het gebruik van STIX en TAXII. Het bezitten en verspreiden van kennis over gebruik van de standaard wordt als verantwoordelijkheid van de leveranciers van securitysystemen/platformen gezien. Tegelijkertijd lijkt het advies nog steeds relevant doordat onder andere gemeenten en waterschappen niet of nauwelijks gebruik maken van de standaard. Bovendien wordt de standaard niet altijd (juist) gebruikt of weet men niet van het potentieel wat de standaard, naast informatie-uitwisseling, kan bieden.
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	Dit is volgens de experts niet gebeurd. Het advies lijkt nog steeds relevant aangezien gemeenten en waterschappen niet of nauwelijks gebruik maken van de standaard. Bovendien wordt de standaard

	doen over de meerwaarde en toepassing van de uitwisseling van gestructureerde dreigingsinformatie met STIX en TAXII.	niet altijd (juist) gebruikt of weet men niet van het potentieel wat de standaard, naast informatie-uitwisseling, kan bieden.
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.	Dit is volgens de experts niet gebeurd. Wel wordt er uitleg gedeeld over dreigingsinformatie. Experts tonen geen interesse of behoefte in het delen van informatie over de meerwaarde en best practices. Tegelijkertijd lijkt het advies nog steeds relevant doordat onder andere gemeenten en waterschappen niet of nauwelijks gebruik maken van de standaard. Bovendien wordt de standaard niet altijd (juist) gebruikt of weet men niet van het potentieel wat de standaard, naast informatie-uitwisseling, kan bieden.
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).	Hier was sprake van maar staat nu stil doordat het betreffende contract is ontbonden. Het advies is nog steeds relevant doordat gemeenten en waterschappen op dit moment niet of nauwelijks gebruik maken van de standaarden.

Tabel 4 - Status adoptieadviezen

3.2.7. Lopende ontwikkelingen

De experts geven aan dat het onderwerp cyberdreiging/cybersecurity en de markt rondom cyberdreigingsinformatie steeds groter wordt. Het is een belangrijke ontwikkeling die steeds meer impact heeft in de wereld. Meer en meer organisaties worden met dreigingen of zelfs aanvallen geconfronteerd. De Nederlandse Cybersecuritystrategie 2022-2028 schetst hetzelfde beeld: “De digitale dreiging is permanent en neemt eerder toe dan af, met alle mogelijke gevolgen van dien.”. Een van de geïdentificeerde uitdagingen met betrekking tot de digitale weerbaarheid van de afgelopen jaren is dat informatie-uitwisseling gefragmenteerd is, waardoor dreigingsinformatie niet altijd alle organisaties tijdig bereikt en organisaties niet tijdig in staat worden gesteld om maatregelen te treffen.

Cybersecurity is een vakgebied in ontwikkeling, er is veel beweging maar het is moeilijk om te voorspellen waar het heen gaat. Het is goed denkbaar dat er nieuwe ontwikkelingen komen die de standaard overbodig zullen maken, maar vooralsnog is hier geen sprake van.

3.3. Conclusies en aanbevelingen TAXII

3.3.1. Conclusies TAXII

De meest opvallende conclusie is het ontbreken van een regierol vanuit de Nederlandse overheid op de TAXII standaard, voor zover deze evaluatie dit kon achterhalen (zie ook paragraaf 3.2 Evaluatie van TAXII). Er is geen betrokkenheid vanuit de Nederlandse overheid bij de beheerorganisatie OASIS. Enkele van de bevindingen hieronder zijn het gevolg van het ontbreken van deze regierol.

Toepassingsgebied

Het toepassingsgebied is correct geformuleerd. Een enkele opmerking over een aanscherping geeft geen aanleiding om de formulering van het toepassingsgebied te herzien.

Toegevoegde waarde

De toegevoegde waarde van de TAXII standaard staat niet ter discussie. Voor de overheidspartijen lijkt het vanzelfsprekend te zijn dat er in een situatie met toenemende cyberdreigingen een standaard is die de uitwisseling van cyberdreigingsinformatie faciliteert. De werking van de standaard staat in de basis niet ter discussie, wel zijn er ervaringen die opgepakt worden door de TAXII subcommittee ter verbetering van de standaard.

Het potentieel van de TAXII standaard om te komen tot snelle en geautomatiseerde reacties op aanvallen is niet altijd bekend bij overheidspartijen.

Draagvlak

De adoptie van de standaard op rijksniveau is hoog. De meeste experts schrijven het succes toe aan de leveranciers die de standaard implementeren in hun producten. Het draagvlak van de standaard op rijksniveau is groot, ook de adoptie door de markt is groot. Een kanttekening is het lage adoptieniveau door gemeenten en waterschappen.

Overheidspartijen zijn afhankelijk van de leveranciers in de werking van de standaard en in welke versie van de standaard wordt gebruikt. Experts geven aan dat de adoptie van de nieuwe versie achterblijft, mede doordat leveranciers nog niet allemaal over zijn op de nieuwe versie.

Het NCSC gebruikt beide versies van de standaard. Dit geeft geen signaal of motivatie aan anderen om de nieuwe versie van de standaard te adopteren, waardoor de adoptie van de nieuwe versie niet bevorderd wordt.

Beheer

De standaard wordt actief beheerd, door OASIS. Daarentegen is er geen regierol vanuit de Nederlandse overheid op de TAXII standaard. De aanmelder van de standaard, NCSC, heeft niet of nauwelijks contact met de beheersorganisatie. Er is geen aansluiting bij OASIS vanuit de Nederlandse overheid.

Opname op de ‘pas toe of leg uit’-lijst

Alle bevraagde experts beamen dat de standaard, en met name de nieuwe versie TAXII 2.1, opgenomen moet worden op de ‘pas toe of leg uit’-lijst. Dit biedt overheidspartijen een formele grondslag en extra motivatie om de nieuwe versie van de standaard uit te vragen. Tegelijkertijd schrijven de bevraagde experts de hoge adoptiegraad toe aan de leveranciers van securitysystemen/platformen die de standaard in hun systemen implementeren. Deze leveranciers zijn de drijvende kracht in de adoptie van de

standaard, maar kunnen wel beïnvloed worden door een sterk signaal vanuit de Nederlandse overheid zoals de opname op de ‘pas toe of leg uit’-lijst.

Status adoptieadviezen

De adoptieadviezen zijn niet of nauwelijks opgevolgd. De regie mist op deze standaard hetgeen eraan bijdraagt dat opvolging van adoptieadviezen nergens landt. De bevraagde experts geven geen signalen dat er behoefte is aan kennisdeling, workshop of best practices. Tegelijkertijd is te zien dat de adoptie in sectoren achter blijft, zoals bij gemeenten en waterschappen, waardoor de gestelde adoptieadviezen nog steeds relevantie hebben.

Lopende ontwikkelingen

De lopende ontwikkelingen tonen dat cyberdreigingen steeds relevanter worden en dat de markt hieromheen toeneemt. De standaarden spelen hier een belangrijke rol in. Vooralsnog worden er geen ontwikkelingen voorzien die dit zouden veranderen.

3.3.2. Aanbevelingen TAXII

Vanuit de analyse van de interviews en de bovenstaande conclusies zijn de volgende aanbevelingen opgesteld aan het Forum standaardisatie:

1. In gesprek gaan met het NCSC over de regierol op de TAXII standaard gezien het NCSC de aanmelder van de TAXII standaard op de ‘pas toe of leg uit’-lijst is geweest.

2. In samenwerking met het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties afdeling Digitale Samenleving onderzoeken waar de regierol voor de TAXII standaard binnen de Nederlandse overheid het beste is belegd en hierover adviseren.

3. De markt rondom cyberdreigingsinformatie groeit en is in beweging. De kans dat er op een middellange termijn ontwikkelingen zijn die de standaarden raken is groot. Het advies is om tussen de twee en vier jaar de standaard opnieuw te evalueren.

Zodra de regierol voor de TAXII standaard belegd is binnen de Nederlandse overheid dan zijn de volgende aanbevelingen aan de partij die de regierol op zich neemt gericht:

4. Contact leggen met partijen die actief zijn in de TAXII subcommittee bij de beheerorganisatie OASIS met als doel om zicht en grip te krijgen op het beheerproces en op internationale ontwikkelingen.

5. Opnieuw onderzoeken van het nut en de noodzaak van de adoptieadviezen. De experts geven geen signalen dat er behoefte is aan kennisdeling over de standaard. Daarentegen loopt de adoptie bij gemeenten en waterschappen achter en is de potentiële meerwaarde van de standaard niet helder voor alle organisaties.

6. Uitdragen en communiceren van toegevoegde waarde van de TAXII standaard.

7. Onderzoek in hoeverre er sprake is van leveranciersafhankelijkheid bij de TAXII standaard door de sterke rol van leveranciers in de ontwikkeling en het uitdragen van de standaard.

4. Algemene conclusie en aanbevelingen

4.1. Conclusies en aanbevelingen over cluster ‘Veilig internet’

De STIX en TAXII standaarden zijn niet de enige standaarden die binnen het cluster ‘Veilig internet’ vallen. Het zijn wel de enige standaarden die zich specifiek richten op de uitwisseling van cyberdreigingsinformatie.

De bevraagde experts geven aan dat STIX en TAXII duidelijk twee verschillende standaarden zijn, en dat ze ook zodanig behandeld dienen te worden. Tegelijkertijd geven ze aan dat de standaarden nauwelijks apart van elkaar gebruikt worden.

Op de ‘pas toe of leg uit’-lijst staan beide standaarden nu als één standaard opgenomen. Op dit moment leidt het niet tot verwarring of problemen bij gebruikers van de standaarden. Mocht er gekozen worden op de standaarden afzonderlijk op de lijst te plaatsen dan is de aanbeveling om de toepassingsgebieden van de standaarden te herzien.

4.1.1. Conclusie en aanbeveling voor alle standaarden

Het ontbreken van de regierol bij de Nederlandse overheid geldt voor STIX en TAXII. Aangezien STIX en TAXII niet de enige standaarden zijn in het cluster ‘Veilig internet’ en de overige standaarden niet binnen deze evaluatie vallen kunnen we niet concluderen dat dit ook voor de andere standaarden geldt. Wel kunnen we concluderen dat het van belang is om voor iedere standaard op de ‘pas toe of leg uit’-lijst en nieuw aangemelde standaarden na te gaan of de regierol belegd is. Dit is van belang voor het houden van zicht en grip op het beheerproces, het aansluiten op internationale ontwikkelingen en het opvolgen van de adoptieadviezen.