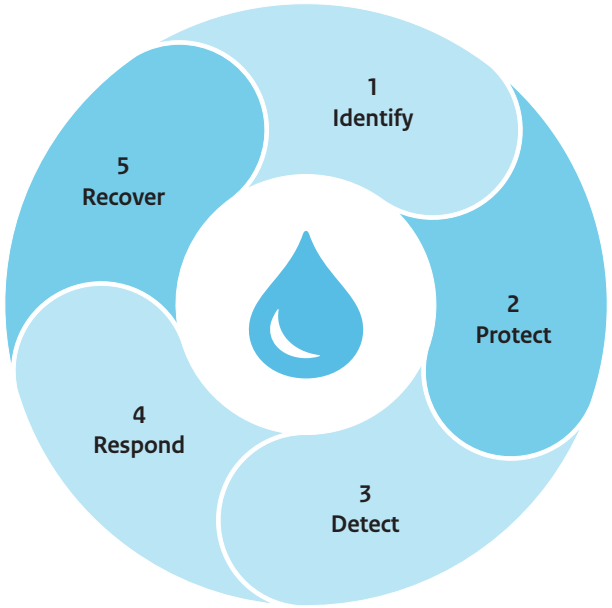
Thema

Trainen, Testen en Oefenen (TTO)

De impact van cyberincidenten kan kleiner worden door effectief te trainen, testen en oefenen. Trainen en oefenen zorgen voor bewustzijn en continue verbetering. Testen geeft inzicht in de maatregelen die genomen zijn. Het laat bovendien zien of deze maatregelen de organisatie in de praktijk weerbaar maken tegen cyberaanvallen. Blijkt dit niet (voldoende) het geval, dan laat testen zien welke verbeterpunten nodig zijn.

Doel

1. Impact van cyberincidenten minimaliseren door optimaal voorbereid te zijn.
2. Identificeren van verbeterpunten voor de cyberweerbaarheid van organisaties.
3. Organisaties en medewerkers van verschillende organisaties weten elkaar te vinden en het uitwisselen van kennis wordt gestimuleerd.



Verwijzing naar bestaande documenten

- Cyberoefening ISIDOOR | Nationaal Cyber Security Centrum (ncsc.nl)
- CVD-beleid inrichten | Nationaal Cyber Security Centrum (ncsc.nl)
- Whitepaper Pen-testen doe je zo | Whitepaper | Nationaal Cyber Security Centrum (ncsc.nl)
- Whitepaper Red teaming in de praktijk (digitaleoverheid.nl)
- TIBER: samen tegen cybercrime (dnb.nl)

Doelgroep: Alle soorten medewerkers binnen een organisatie. Hoe hoger de cybervolwassenheid van de organisatie, hoe meer behoefte er is aan complexere oefenscenario's en voorzieningen.

Fase NIST framework:
Protect, Recover

Ministerie van Infrastructuur en Waterstaat

Programma Versterken Cyberweerbaarheid in de watersector

Instrumenten niveau 1

Basis

Voor organisaties die af en toe meedoen aan oefeningen zoals ISIDOOR en/of sporadisch een pentest doen

Serious game cybercrisis ★ ⚙

Bekijk de trailer hier

Kijk mee met het fictieve drinkwaterbedrijf 'Alisson'. Deze game helpt medewerkers hun kennis en handelingsperspectief bij een cybercrisis te vergroten. Terwijl zich een cyberincident ontvouwt, wordt al spelenderwijs duidelijk waar de verbeterpunten liggen in de eigen organisatie. Beschikbaar voor alle organisaties in de watersector. Het is ook mogelijk deze game aan te passen voor specifieke doelgroepen of organisaties.

Complexiteit instrument

Niveau 2

Voor organisaties die een test- en oefenbeleid (OTO-beleid) hebben en meerdere keren per jaar op structurele wijze oefenen

Zie niveau 1 +

Red Team Blue Team training ★ ⚙

RTBT-training

Deze RTBT-training leert iedereen die werkt met OT-systemen (Operationele Technologie-systemen) de fundamenten van cybersecurity. De deelnemers krijgen inzicht in offensieve en defensieve maatregelen. Ook gaan ze zelf aan de slag. Leden van het blauwe team verdedigen hun netwerk, bestaande uit OT-componenten, terwijl het rode team het netwerk aanvalt. In 2022 vindt deze training twee keer plaats. Ook wordt de training dit jaar aangepast om beter aan te sluiten op OT-omgevingen in de watersector.

Serious game ketenafhankelijkheden ⚙

Oefeningen met meerdere organisaties in de keten. Bij deze game wordt geoefend met incidentscenario's die meerdere organisaties in de keten raken. De nadruk ligt op het verkleinen van de impact van deze ketenincidenten. Het gaat om laagdrempelige oefeningen die een beperkte voorbereiding vragen. Bij voorkeur vinden de oefeningen plaats n.a.v. een vooraf uitgevoerde ketenanalyse.

Complexiteit instrument

Niveau 3

Voor organisaties die monitoring hebben ingericht *(bijv. m.b.v. een Security Operations Center (SOC))*, een test en oefenbeleid hebben en meerdere keren per jaar op structurele wijze oefenen

Zie niveau 1 + niveau 2 +

Haalbaarheidsstudie Cyber range oefenfaciliteit ⚙

Oefenen met realistische aanvalsscenario's in een omgeving die lijkt op de eigen systeemomgeving en waarin ook objecten zijn opgenomen: het kan de cyberweerbaarheid flink verhogen. Daarom onderzoekt het Programma Versterken Cyberweerbaarheid in de Watersector samen met onderzoeksinstituten en stakeholders uit de watersector de mogelijkheden voor een cyber range oefenfaciliteit water. In een cyber range omgeving kunnen cybersecurity specialisten offensieve en defensieve vaardigheden oefenen.

Red teaming testmethode ⚙

Ontwikkeling van een redteaming methode toepasbaar in de watersector. Door red team testen, gebaseerd op realistische dreigingen, krijgen organisaties inzicht in hun sterke en zwakke punten. Ook vergroten ze zo hun weerbaarheid tegen geavanceerde cyberaanvallen. Organisaties in de watersector kunnen deze manier van testen gaan gebruiken en resultaten met elkaar delen. Hierdoor vergroten ze ook de gezamenlijke weerbaarheid. Het Programma Versterken Cyberweerbaarheid in de Watersector begeleidt hen bij de ontwikkeling van de redteaming methode en het uitwisselen van resultaten.

Legenda: ★ *beschikbaar* ⚙ *nog te ontwikkelen/verder ontwikkelen*

Ministerie van Infrastructuur en Waterstaat

Programma Versterken Cyberweerbaarheid in de watersector

Thema

Ketens en Risico-management (KR)

Voor een goede besturing van watersystemen is het belangrijk om inzicht te hebben in de risico's. Dit geldt ook voor het inzicht in de onderlinge afhankelijkheden binnen waterketens. Een (cyber)incident bij één organisatie kan immers ook digitale of fysieke gevolgen hebben voor andere organisaties. Dat inzicht begint bij het inventariseren van de vitale objecten en mogelijke risico's. De instrumenten die bij dit thema horen, richten zich op de keten als geheel.

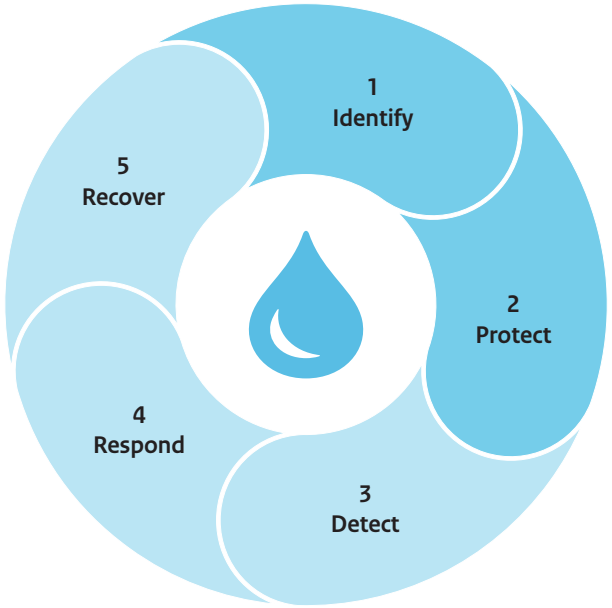
Doel

Inzicht hebben in de risico's die voor een organisatie relevant zijn:

1. Classificeren van objecten (op basis van Business Impact).
2. Uitvoeren van ketenanalyses.
3. Inventariseren welke cybersecurity risico's relevant zijn voor de organisatie.

Verwijzing naar bestaande documenten

- Onderzoek Cyber Security Raad naar supply chain methodiek (cybersecurityraad.nl)
- Analyse van TNO over soorten ketens (ncsc.nl)
- NCSC risicomanagement (ncsc.nl)
- NCSC Trendlijst 2021 (ncsc.nl)



Doelgroep: Risicomanagers, assetmanagers, procesdeskundigen, beleidsmedewerkers cybersecurity en bestuurders.

Fase NIST framework:
Identify, Protect

Ministerie van Infrastructuur en Waterstaat

Programma Versterken Cyberweerbaarheid in de watersector

Complexiteit instrument

Niveau 1

Voor organisaties die nog niet structureel aan cybersecurity risicomanagement doen.

Handreiking risicoanalyse OT security

Deze handreiking heeft als doel bestuurders in staat te stellen beter in kaart te hebben welke cybersecurity risico's voor hun organisatie relevant zijn en waar sturing nodig is.

Inzicht in dreigingen watersector

Op basis van een algemeen strategisch dreigingsbeeld wordt specifiek voor de watersector een dreigingsbeeld opgesteld. Dit wordt vertaald naar een operationeel niveau waardoor gerichter maatregelen genomen kunnen worden die proportioneel en adequaat zijn.

Handreiking classificeren missiekritieke objecten

De Handreiking classificeren missiekritieke objecten is ontwikkeld voor de Nederlandse waterschappen. Ze geeft hun een methode waarmee zij zélf hun processen, objecten en systemen kunnen beoordelen. Zo kunnen ze bepalen welke processen, objecten en systemen essentieel zijn voor het continueren van het proces 'keren en beheren waterkwantiteit'.

Actualiseren weerbaarheidsanalyse en actie-programma 'keren en beheren waterkwantiteit'

Het proces keren en beheren waterkwantiteit wordt conform de vereisten vanuit de NCTV opnieuw beoordeeld op vitaliteit. Op basis van de uitkomsten worden maatregelen voor de versterking van de cyberweerbaarheid van het proces geïdentificeerd. In de weerbaarheidsanalyse en het actieprogramma komen vervolgens aanbevelingen om deze maatregelen ook in te voeren in de praktijk.

Complexiteit instrument

Niveau 2

Voor organisaties die structureel aan cybersecurity risico-management doen.

Zie niveau 1 +

Ontwikkelen methode ketenanalyse

Ontwikkelen van een methode voor het uitvoeren van ketenanalyses binnen de watersector. De 'Cyber security supply chain risk analysis' van de Cyber Security Raad (CSR) vormt de basis voor deze methode. Het doel van de methode is om cybersecurityrisico's voor de keten als geheel in kaart te brengen. De ketenanalyse methode voor de watersector is getoetst in drie casestudies. Hierbij zijn drinkwaterbedrijven, waterschappen, gemeenten en Rijkswaterstaat betrokken.

Complexiteit instrument

Niveau 3

Voor organisaties die structureel aan risicomanagement doen en hierbij ketenanalyses toepassen.

Zie niveau 1 + niveau 2 +

Ketenanalyse hoofd- en regionale watersystemen

Samen met RWS en de waterschappen wordt de methodiek voor ketenanalyse toegepast in het hoofdwatersysteem en alle regionale watersystemen. Hiermee worden voor de hele keten onderlinge afhankelijkheden en risico's inzichtelijk. Ook bevordert dit de samenwerking op het gebied van cybersecurity. Dit is tevens input voor het project actualiseren weerbaarheidsanalyse en actieprogramma 'keren en beheren waterkwantiteit''.

Legenda: ★ *beschikbaar* ⚙ *nog te ontwikkelen/verder ontwikkelen*

Ministerie van Infrastructuur en Waterstaat

Programma Versterken Cyberweerbaarheid in de watersector

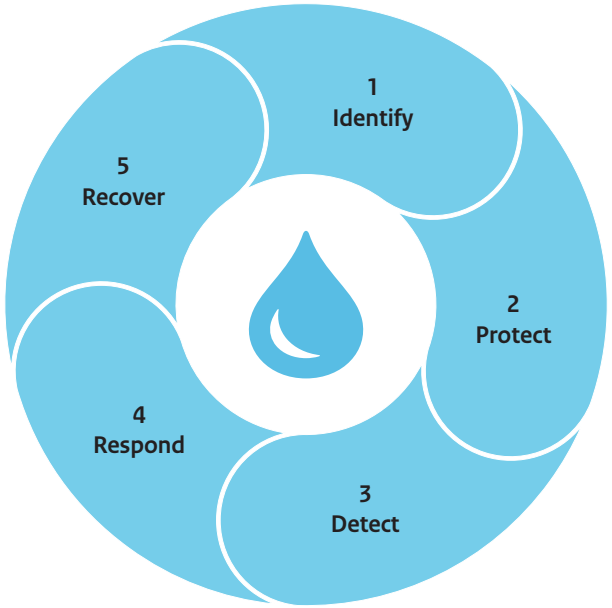
Thema

Maatregelen en Implementatie (MI)

Dit thema ondersteunt organisaties om de juiste maatregelen te treffen. Zij zijn zelf verantwoordelijk voor deze maatregelen. De projecten binnen dit thema richten zich specifiek op het aanreiken van middelen om eenvoudiger de relevante maatregelen te nemen voor vitale processen en proces-automatisering /Operationele Techniek (OT).

Doel

Organisaties optimaal ondersteunen bij het nemen van de (basis-)maatregelen. En daarnaast instrumenten bieden voor het nemen van extra maatregelen die passen bij het risicoprofiel van de organisatie.



Verwijzing naar bestaande documenten

Maatregelen die op basis van de Wbni zijn voorgeschreven:

- Bbni – zie specifiek Bijlage bij artikel 3a (officielebekendmakingen.nl)
- Mrbni (officielebekendmakingen.nl)
- Handreiking Cybersecuritymaatregelen (ncsc.nl)
- ICS weerbaar maken (ncsc.nl)
- Security Check Procesautomatisering (digitaltrustcenter.nl)
- CSIR (cip-overheid.nl)

Doelgroep:
Risicomanagers, beleidsmedewerkers, CISO's, functioneel beheerders.

Fase NIST framework:
Identify, Protect, Detect, Respond, Recover

Ministerie van Infrastructuur en Waterstaat

Programma Versterken Cyberweerbaarheid in de watersector

Complexiteit instrument

Niveau 1

Voor organisaties die ondersteuning zoeken bij het identificeren van de juiste maatregelen.

Adviesdag Ransomware preparedness (RAP)

Met dit instrument van een dag of dagdeel krijgen deelnemers laagdrempelig advies over ransomware.

Workshop OT security

Kennis van OT is schaars, ook binnen organisaties die veel werken met OT. In deze workshop frissen deelnemers hun basiskennis op. Maar ze doen ook nieuwe kennis op, bijvoorbeeld aan de hand van best practices. Verder zijn ze na de workshop bij op het gebied van normen zoals de Cybersecurity implementatierichtlijn (CSIR) en IEC62443.

Best practises Kwetsbaarheden- en patchmanagement

Dit jaar wordt een webinar georganiseerd dat inzoomt op de specifieke eigenschappen van het patchproces in OT-omgevingen. De hoofdlijnen van deze webinar worden ook beschikbaar gesteld in een korte whitepaper.

Handreiking industriële automatisering en controle systemen secure (HIACSS)

Deze handreiking helpt organisaties bij het implementeren van OT security maatregelen. In dit document wordt ook de verbinding gelegd met de BIO (en ISO27002). Daarmee fungeert het als opstapje naar de uitgebreidere CSIR 3.0

Handreiking proces Coordinated Vulnerability Disclosure (CVD)

Niet alle organisaties hebben een gedocumenteerd ‘Coordinated Vulnerabilty Disclosure’ (CVD) proces. Met zo’n proces kunnen buitenstaanders kwetsbaarheden melden. Er wordt in overleg met de organisaties in de watersector een handreiking opgesteld.

Complexiteit instrument

Niveau 2

Voor organisaties die bekend zijn met de basismaatregelen en meer willen doen aan OT security.

Zie niveau 1 +

Verbreding Cyber Security Implementatie Richtlijn voor Waterschappen (CSIR 3.0)

Rijkswaterstaat en de waterschappen hebben de Cybersecurity implementatierichtlijn (CSIR 3.0) ontwikkeld. De CSIR 3.0 is een optioneel kader met een passende set beheersmaatregelen die de vitale infrastructuur met industriële automatisering cyberweerbaar maakt en houdt. Het document onderscheidt zich van de op IV gerichte BIO. De CSIR 3.0 bevat vanuit de Europese standaard voor beveiliging OT, de IEC 62443 aanvullende eisen en maatrege len om de risico’s te beheersen in het OT-domein.

Use cases en app CSIR

De CSIR 3.0 wordt toegepast in een aantal use cases bij de waterschappen. Daarnaast wordt tooling ontwikkeld die de maatregelen uit de CSIR op een eenvoudige wijze toegankelijk maakt voor alle organisaties in de watersector en eventueel ook daarbuiten. De tooling helpt daarmee de asseteigenaar om cybersecurity te borgen in de lifecycle en aan te sluiten op bestaande processen.

Complexiteit instrument

Niveau 3

Voor organisaties die het nemen van maatregelen binnen de eigen organisatie goed ingeregeld hebben en aan de slag willen met ketenrisico’s.

Zie niveau 1 + niveau 2 +

Implementatie onderzoeksresultaten ketenanalyse

Deze activiteit richt zich op organisaties die ketenanalyses hebben uitgevoerd. Op basis van de uitkomsten van deze analyse wordt onderzocht welke stappen zij kunnen zetten om passende maatregelen te implementeren en monitoren. Deze maatregelen kunnen de gesignaleerde cybersecurity risico’s in de keten kleiner maken.

Legenda: ★ *beschikbaar* ⚙ *nog te ontwikkelen/verder ontwikkelen*

Ministerie van Infrastructuur
en Waterstaat

Programma
Versterken
Cyberweerbaarheid
in de watersector

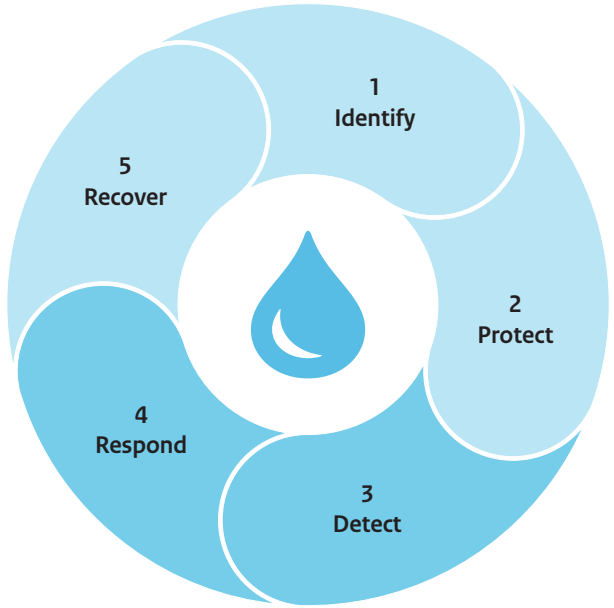
Thema

Monitoring en Detectie (MD)

Het is onmogelijk om cyberincidenten helemaal te voorkomen. Het is daarom belangrijk om afwijkend gedrag binnen de systemen snel te kunnen signaleren. Met de inrichting van cybersecuritymonitoring wordt de status van netwerk- en informatiesystemen (IT en OT) in de gaten gehouden. Hierbij worden relevante gebeurtenissen vastgelegd en wordt afwijkend gedrag herkend om onderzocht te kunnen worden.

Doel

Het optimaal inrichten van monitoring en detectie. Zo kunnen incidenten snel opgemerkt worden. De impact van incidenten kan op deze manier bovendien zo klein mogelijk worden gehouden.

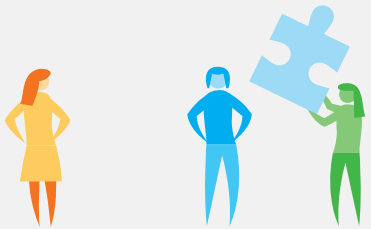


Verwijzing naar bestaande documenten

- Handreiking voor implementatie van detectie oplossingen (ncsc.nl)
- SOC inrichten: begin klein (ncsc.nl)

Doelgroep: Analisten, technisch beheerders en functioneel beheerders.

Fase NIST framework:
Detect, Respond



Ministerie van Infrastructuur en Waterstaat

Programma Versterken Cyberweerbaarheid in de watersector

Complexiteit instrument

Niveau 1

Voor organisaties die weinig of alleen basismonitoring ingericht hebben.

Workshop best practices monitoring en detectie ⚙

Organisaties die nog niet de ambitie of de mogelijkheid hebben om een Security Operations Center (SOC) op te zetten, ontplooien vaak wel andere activiteiten op het gebied van detectie en monitoring. Deze workshop neemt deelnemers van deze organisaties mee langs een aantal best practices. Dit helpt hen om monitoring en detectie optimaal in te richten binnen hun organisatie en quick wins te realiseren.

Complexiteit instrument

Niveau 2

Voor organisaties die monitoring hebben ingericht inclusief bijbehorende processen.

Zie niveau 1 +

Haalbaarheidsstudie SOC watermanagement ★ ⚙

Haalbaarheidsstudie naar het leveren van een monitorings-dienst vanuit de samenwerking CERT-WM/SOC-RWS aan waterschappen door middel van een proof-of-concept (PoC). In deze pilot wordt aansluiting getoetst langs de lijnen techniek, processen, organisatie en mensen.

Verkenning samenwerking monitoring en detectie watersector ⚙

Het Programma Versterken Cyberweerbaarheid in de Watersector onderzoekt samen met de watersector of samengewerkt kan worden op het gebied van monitoring en detectie.

Complexiteit instrument

Niveau 3

Voor organisaties die een SOC hebben ingericht of dit op korte termijn opstarten.

Zie niveau 1 + niveau 2 +

Legenda: ★ *beschikbaar* ⚙ *nog te ontwikkelen/verder ontwikkelen*

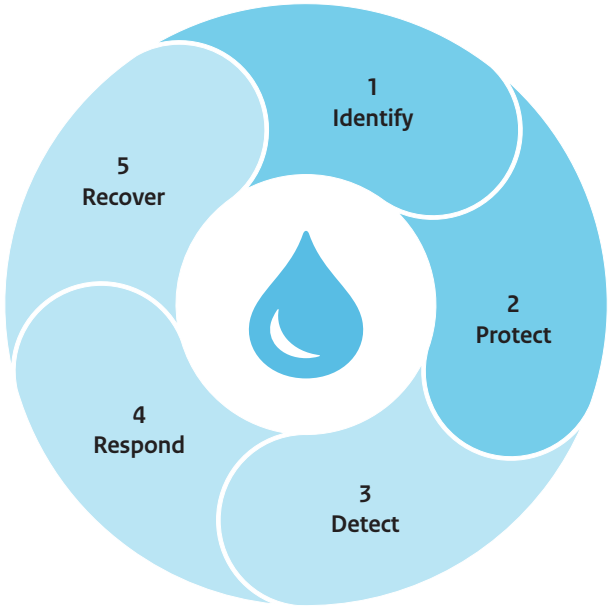
Thema

Samenwerking en Expertise (SE)

Het Programma Versterken Cyberweerbaarheid in de Watersector geeft uitvoering aan de aanvullende afspraken uit het 'Bestuursakkoord Water' van 2018. Sindsdien is de samenwerking op het gebied van cybersecurity en OT-security in het bijzonder aanzienlijk gegroeid. Het is wenselijk om deze samenwerking ook op lange termijn voort te zetten. De ontwikkelde kennis en kunde moeten bovendien behouden blijven. Duurzame borging van alle expertise is dan ook het kerndoel van dit thema.

Doel

De cybersecurityexpertise binnen de watersector verbeteren door het verstevigen van de samenwerking en het borgen van de kennis.



Verwijzing naar bestaande documenten

- Bestuursakkoord Water (helpdeskwater.nl)

Doelgroep:
Bestuurders, beleidsmedewerkers, kenniscoördinatoren.

Fase NIST framework:
Identify, Protect

Ministerie van Infrastructuur en Waterstaat

Programma Versterken Cyberweerbaarheid in de watersector

Complexiteit instrument

Niveau 1

Voor organisaties die actiever willen samenwerken met de sector maar nog zoeken naar een invulling daarvan.

Faciliteren en borgen bestuurlijke afspraken ⚙

De aanvullende afspraken uit het Bestuursakkoord Water lopen eind 2022 af. Daarom wordt in de loop van 2022 bezien of, en zo ja in welke hoedanigheid, verlenging van de samenwerking mogelijk en wenselijk is.

ONE conference water en OT track ⚙

Voor het uitwisselen van kennis en expertise worden enkele kennissessies georganiseerd tijdens de ONE conference van het NCSC. Onder andere een grote serious game sessie staat op het programma.

Complexiteit instrument

Niveau 2

Voor organisaties die willen aansluiten bij sectorale samenwerking op het gebied van cybersecurity.

Zie niveau 1 +

Uitbouwen CERT-WM functionaliteit ⚙

In 2020 is een analyse uitgevoerd naar de SOC- en CERT-functie binnen RWS en de waterschappen. Er wordt een actieplan opgesteld om de robuustheid te verbeteren. Dit actieplan sluit aan bij de ambities van het CERT-WM en waarborgt het uitwisselen van informatie en kennisproducten voor de watersector.

Complexiteit instrument

Niveau 3

Voor organisaties die actief willen en kunnen bijdragen aan het vergroten van het kennisniveau binnen de watersector.

Zie niveau 1 + niveau 2 +

Center of expertise ⚙

In 2022 wordt nader bezien of centrale borging nodig is voor de opgebouwde expertise en samenwerkingsvormen. Uitgangspunt hiervoor zijn de projecten binnen de vijf thema's en de nieuw te ontwikkelen programmawebsite. Het gaat dan ook om een groeimodel. Daarnaast zal aansluiting worden gezocht bij de IenW-brede cybersecurity strategie.

Legenda: ★ *beschikbaar* ⚙ *nog te ontwikkelen/verder ontwikkelen*