Programma

Versterken Cyberweerbaarheid in de watersector

Jaarplan 2023 –2024
Projecten

Contact
www.versterkencyberweerbaarheid.nl
cyberweerbaarheidwater@minienw.nl

Ministerie van Infrastructuur en Waterstaat

Programma Versterken Cyberweerbaarheid in de watersector

Overzicht projecten

Trainen, testen en oefenen

- Bestuurlijke cybercrisis oefening - OT
- Curriculum trainingen
- Serious game cybercrisis
- Red Team / Blue Team training
- Serious game ketenafhankelijkheden
- Haalbaarheidsstudie cyberrange oefenfaciliteit
- TIBER water
- Red teaming testmethode

Ketens en risicomanagement

- Handreiking en workshop 'Grip op aanvalsoppervlak'
- Inzicht in dreigingen watersector (periodiek)
- Handreiking classificeren missiekritieke objecten
- Verkennen gedeelde afhankelijkheden toeleveranciers
- Methode ketenanalyse
- Ketenanalyse hoofd- en regionaal watersysteem

Maatregelen en implementatie

- Aandachtspunten implementatie NIS2
- Stimuleren implementatie 'Responsible Disclosure (RD)'
- Webinair en paper beschermen logdata
- Adviesdag Ransomware Preparedness (RAP)
- Best practices kwetsbaarheden- en patchmanagement
- Handreiking Basismaatregelen voor cybersecurity van IACS (BIACS)
- Inrichten beheer en onderhoud CSIR
- CSIR Tooling
- Verbreding Cyber Security Implementatie Richtlijn voor waterschappen (CSIR3.0)
- Ketenregie: uitwerken rollen en verantwoordelijkheden
- Implementatie ketenmaatregelen

Monitoring en detectie

- Seminar best practices monitoring en detectie
- Handreiking 'Opvolging cybersecurity meldingen'
- Ondersteunen SOC waterschappen
- Monitoring en detectie drinkwatersector
- Haalbaarheidsstudie SOC watermanagement
- Haalbaarheidsstudie scannen op kwetsbaarheden binnen de sector

Samenwerking en expertise

- Borging resultaten programma
- Bestuurlijk commitment vergroten
- Gezamelijke visie en ambitie bepalen
- Versterken programma governance
- ONE Conference 2023
- ONE Conference 2022 OT-track
- Doorontwikkeling CERT-stelsel watersector
- Uitbouwen CERT-WM functionaliteit
- Center of Expertise

Legenda:

- *Complexiteit instrument | Basis*
- *Complexiteit instrument | Gevorderd*
- *Complexiteit instrument | Volwassen*
- *Nieuw of verder te ontwikkelen*
- *Beschikbaar*

Thema

Trainen, Testen en Oefenen

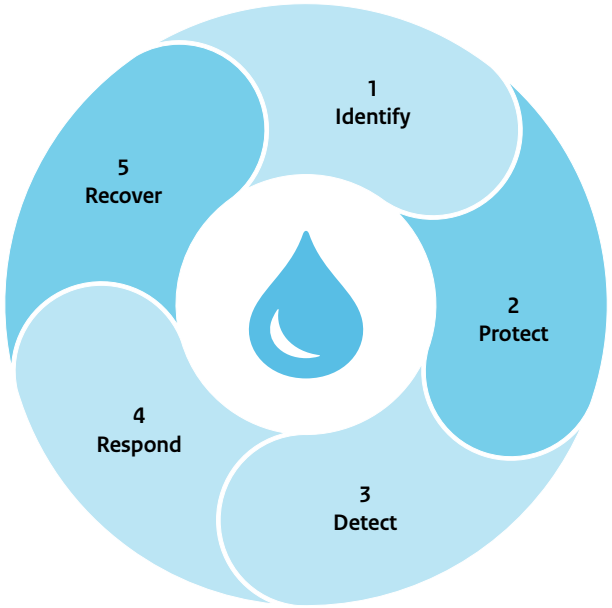
De impact van cyberincidenten kan kleiner worden door effectief te trainen, testen en oefenen. Trainen en oefenen zorgen voor bewustzijn en continue verbetering. Testen geeft inzicht in de maatregelen die genomen zijn. Het laat bovendien zien of deze maatregelen de organisatie in de praktijk weerbaar 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.

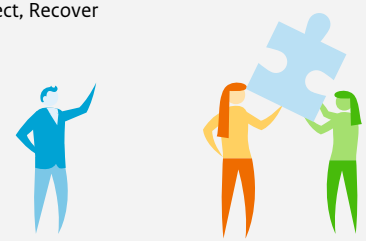
Meer informatie?

Wil je meer weten over dit thema binnen de watersector bekijk onze webpagina Trainen, Testen en Oefenen (TTO). Voor eventuele vragen over dit thema kunt u contact opnemen via cyberweerbaarheidwater@minienw.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



Trainen, Testen en Oefenen | ⚙ Nieuw of verder te ontwikkelen

Complexiteit instrument
Basis

Bestuurlijke cybercrisis oefening – OT

Na de ISIDOOR-oefening presenteren we tijdens een bestuurlijke cybertafel een ISIDOOR 'light' scenario op maat. Het doel is om bestuurders zelf te laten oefenen en inzichten te geven in de resultaten van de volledige ISIDOOR-oefening.

Curriculum trainingen

Naast de bestaande Red Team/Blue Team training die behouden blijft, organiseren we een aanvullende training. In de training bouw je een curriculum op, wat ook voor minder technische OT-specialisten of geïnteresseerden toegevoegde waarde biedt.

Complexiteit instrument
Gevorderd

–

Complexiteit instrument
Volwassen

Haalbaarheidsstudie Cyber range oefenfaciliteit

Dit onderzoek analyseert de huidige toepassingen van cyberranges en digital twins in de watersector, en identificeert mogelijkheden voor toekomstige toepassing binnen de sector.

TIBER water

De watersector heeft het programma TIBER WATER ontwikkeld. Het programma zal de toepassing van TIBER WATER stimuleren in de sector. Organisaties kunnen met ondersteuning vanuit het programma beginnen met plannen, voorbereiden en uitvoeren van testen. Daarnaast zal het programma een White Team Lead meeting faciliteren die het delen van ervaringen tussen organisaties mogelijk maakt.

Trainen, Testen en Oefenen | ★ Beschikbaar

Complexiteit instrument
Basis

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
Gevorderd

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
Volwassen

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.

Thema

Ketens en Risicomanagement

Voor een goede besturing van watersystemen is het belangrijk om inzicht te hebben in de dreigingen en 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, dreigingsscenario's en mogelijke risico's. De instrumenten die bij dit thema horen, richten zich op de keten als geheel.

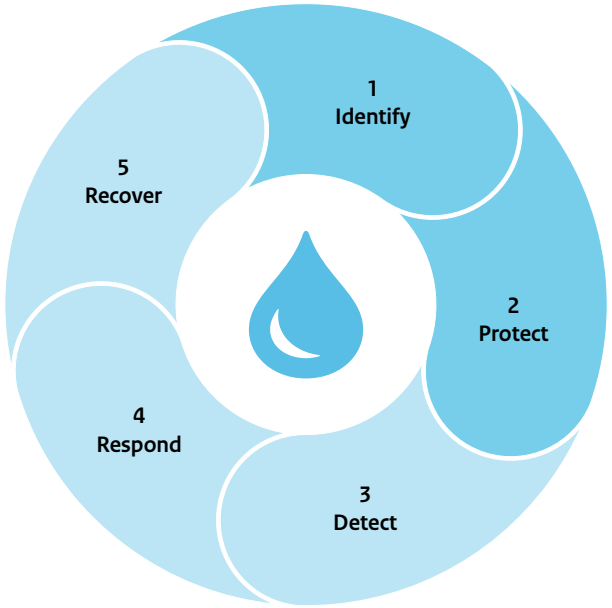
Doel

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.

Meer informatie?

Wil je meer weten over dit thema binnen de watersector bekijk onze webpagina Ketens en Risicomanagement (KR). Voor eventuele vragen over dit thema kunt u contact opnemen via cyberweerbaarheidwater@minienw.nl



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

Fase NIST framework:
Identify, Protect

Ketens en Risicomanagement | ⚙ Nieuw of verder te ontwikkelen

Complexiteit instrument
Basis

Handreiking en workshop ‘Grip op aanvalsoppervlak’

Inzicht hebben in je fysieke en digitale aanvalsoppervlak is essentieel om te kunnen bepalen waar je kwetsbaar bent als organisatie. Deze workshop en hieruit voortvloeiende handreiking helpt om de omvang van het aanvalsoppervlak en het gebruik van aanvalspaden van de organisatie te begrijpen en in te kunnen schatten. In deze workshop is ook aandacht voor bestaande methodieken om inzichtelijk te krijgen welke assets in gebruik zijn.

Inzicht in dreigingen watersector

We richten een proces in dat periodiek inzicht in dreigingen geeft. Op basis van een algemeen strategisch dreigingsbeeld stellen we dreigingsbeelden op die specifiek zijn voor de watersector. Organisaties moeten dit kunnen vertalen naar een operationeel niveau, waardoor zij gerichter maatregelen kunnen nemen die proportioneel en adequaat zijn. Hierbij kunnen ze geleerde lessen uit andere sectoren meenemen.

Complexiteit instrument
Gevorderd

Verkennen gedeelde afhankelijkheden toeleveranciers

Om in te spelen op de toenemende dreiging van aanvallen via toeleveranciers en de eisen uit NIS2.0, verkennen we van welke belangrijke toeleveranciers een gedeelde afhankelijkheid bestaat. Op basis van de verkenning kunnen we vervolgacties formuleren die organisaties helpen de risico’s te verkleinen die voortkomen uit de toeleverancierssketen. Hierbij is het relevant te kijken naar de opbrengst en de relatie met de ketenanalyses. Daarnaast kunnen we bepalen welke onderdelen van belang zijn voor leveranciersmanagement, ook in relatie tot al bestaande instrumenten, zoals het gebruik van de CSIR in de ICO Wizard.

Complexiteit instrument
Volwassen

Ketenanalyse hoofd- en regionale watersystemen

Samen met Rijkswaterstaat en de waterschappen passen we de methodiek voor ketenanalyse toe 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.

Ketens en Risicomanagement | ★ Beschikbaar

Complexiteit instrument
Basis

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'.

Complexiteit instrument
Gevorderd

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
Volwassen

–

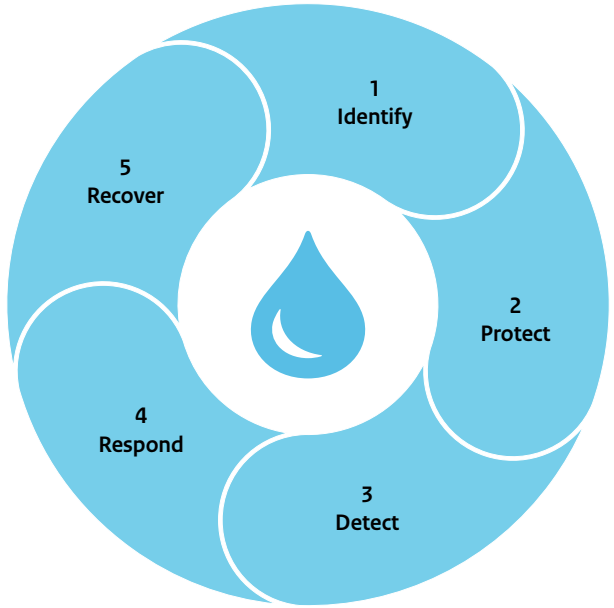
Thema

Maatregelen en Implementatie

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.



Meer informatie?

Wil je meer weten over dit thema binnen de watersector bekijk onze webpagina Maatregelen en Implementatie (MI). Voor eventuele vragen over dit thema kunt u contact opnemen via cyberweerbaarheidwater@minienw.nl

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

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

Maatregelen en Implementatie | ⚙ Nieuw of verder te ontwikkelen

Complexiteit instrument
Basis

Stimuleren implementatie responsible disclosure

Vanuit regelgeving zoals NIS2 en BIO is het een basismaatregel om een responsible disclosure proces te hebben. We maken een self-assessment die een organisatie specifiek beeld geeft van eventuele verbeterkansen, met de mogelijkheid om geautomatiseerd aanbevelingen te ontvangen om dit proces te verbeteren. Uitkomsten zijn niet bedoeld voor IenW om op te sturen.
De self-assessments kunnen periodiek herhaald worden. We kunnen samenwerken met andere sectoren (of bijvoorbeeld NCSC of DTC).

Webinar en paper beschermen logdata

Logdata moet goed afgeschermd zijn om mutatie door kwaadwillenden te voorkomen. Dat vraagt om kennisuitwisseling over opslagvereisten en best practices.

Aandachtspunten implementatie NIS2*

We brengen op een laagdrempelige manier in kaart hoe de instrumenten uit het programma benut kunnen worden voor de vereisten die uit de NIS2 voortvloeien. Daarnaast maken we een globale vergelijking tussen NIS2-vereisten en raamwerken zoals BIO, CSIR en de MR.

** We kunnen dit project kan pas starten als de vereisten uit de zorgplicht zijn vastgesteld.*

Complexiteit instrument
Gevorderd

Inrichten beheer en onderhoud CSIR

Er zijn nu verschillende CSIR-versies voor verschillende doelgroepen in de watersector. De veranderende wet- en regelgeving, zoals de NIS2 en de BIO, en het veranderende cybersecurity dreigingsbeeld met bijbehorende kwetsbaarheden moeten we borgen in de CSIR-kaderstelling. In het project zorgen we dat we dit op een eenduidige wijze vormgeven. Hiermee maken we de formalisatie van de CSIR-versies binnen de watersector voorspelbaar, beheersbaar en controleerbaar.

CSIR-tooling

We maken de huidige tools die ondersteunend zijn aan de CSIR robuuster en stellen deze beschikbaar voor bredere inzet binnen de watersector. Naar behoefte van de operationele omgeving ontwikkelen, beheren en onderhouden we nieuwe tools, producten of diensten (met een koppeling naar de governance van CSIR). Ook werken we aan een raamwerk om vanuit één ISMS te kunnen werken, zodat elk toepassingsgebied (KA/PA/IA/OT) de juiste controls kan hanteren. Deze controls komen zowel uit de BIO of de CSIR om de cybersecurity risico's te kunnen beheersen. Daarbij is het noodzakelijk dat controls zowel uit de BIO als de CSIR nodig zijn die binnen één en dezelfde ISMS gepositioneerd moeten kunnen worden.

Complexiteit instrument
Volwassen

Implementatie ketenmaatregelen

In dit project werken we uit hoe we het nemen van cyberweerbaarheid-verhogende maatregelen op basis van kwetsbaarheden in de keten kunnen vormgeven. We stimuleren het nemen van maatregelen in de keten door afspraken te maken over maatregelen die voortkomen uit de drie ketenanalyses die zijn uitgevoerd.

Ketenregie: uitwerken rollen en verantwoordelijkheden

Er komt een inventarisatie die antwoord geeft op de meer strategische vraag hoe de verantwoordelijkheid in de keten kan worden belegd. Hier kunnen we gebruik van maken in de ketenanalyses die nog uitgevoerd gaan worden. Er is ook een relatie met het vitaalbeleid.

**Dit moeten we bepalen bij de uitwerking in het projectplan: het kan ook een I&W-beleidsrol zijn. Het is een voorwaarde voor de uitvoering van projecten in het programma.*

Maatregelen en Implementatie | ★ Beschikbaar

Complexiteit instrument
Basis

Adviesdag Ransomware preparedness (RAP)

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

Best practises kwetsbaarheden- en patchmanagement

Het belang van een goede digitale weerbaarheid is evident. Niet alleen in informatie verwerkende processen maar ook bij meet- en regelsystemen die voor de aansturing van industriële processen of gebouwbeheersystemen worden gebruikt. Omgevingen waarin deze systemen voorkomen, worden ook wel ‘Industrial Automation and Control Systems’ genoemd. Dit document beschrijft de basismaatregelen voor cybersecurity van IACS-systemen in het OT domein.

Complexiteit instrument
Gevorderd

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 maatregelen om de risico’s te beheersen in het OT-domein.

Complexiteit instrument
Volwassen

–

Thema

Monitoring en Detectie

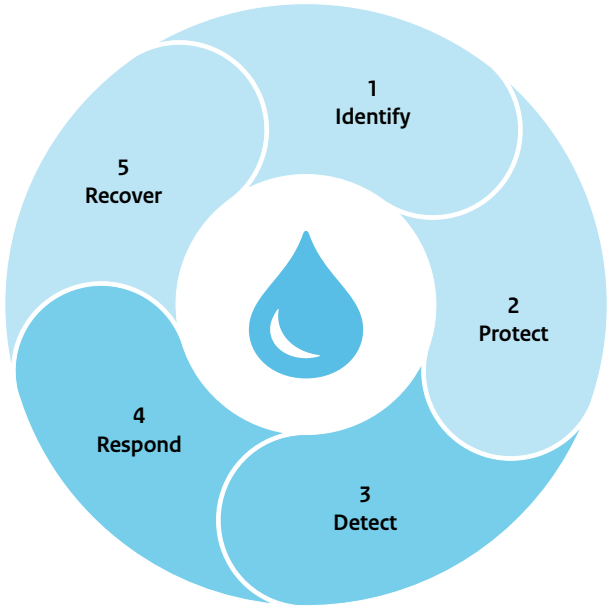
Het is onmogelijk om cyberincidenten helemaal te voorkomen. Het is daarom belangrijk om afwijkend gedrag binnen de systemen snel te kunnen signaleren. Met de inrichting van cybersecuritymonitoring wordt de status van netwerk- en informatiesystemen (IT en OT) in de gaten gehouden. Hierbij worden relevante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

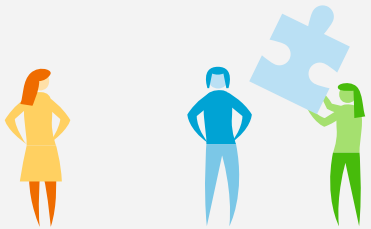
Meer informatie?

Wil je meer weten over dit thema binnen de watersector bekijk onze webpagina Monitoring en Detectie (MD). Voor eventuele vragen over dit thema kunt u contact opnemen via cyberweerbaarheidwater@minienw.nl



Doelgroep: Analisten, technisch beheerders en functioneel beheerders.

Fase NIST framework:
Detect, Respond



Monitoring en Detectie | ⚙ Nieuw of verder te ontwikkelen

Complexiteit instrument
Basis

Seminar best practices monitoring en detectie

In het programma werken we binnen zowel drinkwater als keren en beheren aan roadmaps om monitoring, detectie en de processen die hierop volgen verder te verbeteren. Het project faciliteert met een seminar kennisuitwisseling binnen deze subsectoren. Tijdens dit seminar wisselen we ook uit welke bronnen worden gebruikt voor dreigingsinformatie en wat de ervaringen hiermee zijn.

Handreiking 'Opvolging cybersecurity meldingen'

Het inrichten van een meldingenproces stopt niet bij de melding zelf. Juist het opvolgen van de melding vraagt om een goede procesinrichting en personele capaciteit. Deze handreiking biedt een handvat aan security personeel om hierover binnen de eigen organisatie te spreken. De handreiking is eventueel te combineren met een awareness-sessie of het seminar 'Best practices monitoring en detectie'.

Complexiteit instrument
Gevorderd

Ondersteunen SOC waterschappen

Na de haalbaarheidsstudie PoC SOC geven we een vervolg aan de behoefte die er is vanuit de waterschappen. De nadruk in dit project ligt op de bestuurlijke afstemming over de te bereiken resultaten en de manier waarop we deze resultaten behalen voor monitoring en detectie binnen de waterschappen en de eventuele samenwerking met andere partijen binnen de sector en/of externe partijen.

Monitoring en detectie drinkwatersector

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

Complexiteit instrument
Volwassen

Haalbaarheidsstudie scannen op kwetsbaarheden binnen de sector

Vanuit de NIS2.0 is één van de taken voor een sectoraal CSIRT het scannen op kwetsbaarheden. De vraag is wat binnen de scope van het scannen valt, wat de relatie met hostingpartijen is, hoe ver je hiermee kunt en wilt gaan en hoe het zit met aansprakelijkheid. Het doel is toegevoegde waarde bieden door inzicht te geven aan organisaties die kwetsbaar kunnen zijn. Dit project kan in samenwerking met andere organisaties of CSIRT's worden opgepakt.

Monitoring en Detectie | ★ Beschikbaar

Complexiteit instrument
Basis

–

Complexiteit instrument
Gevorderd

Haalbaarheidsstudie SOC watermanagement

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

Complexiteit instrument
Volwassen

–

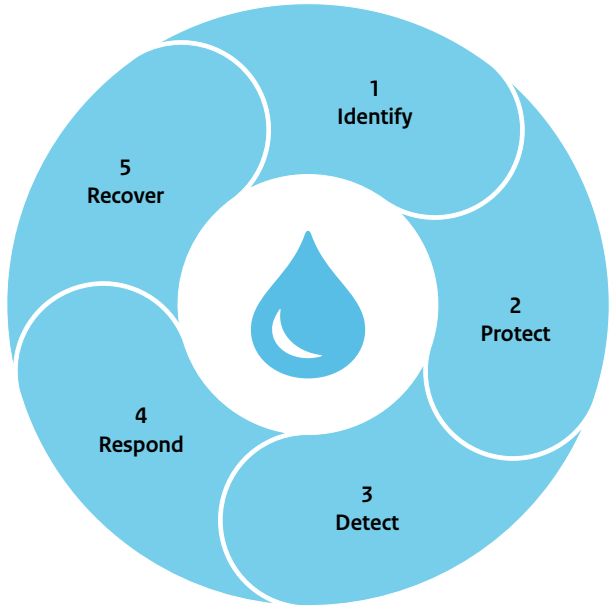
Thema

Samenwerking en Expertise

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.



Doelgroep:
Bestuurders, beleidsmedewerkers, kenniscoördinatoren.

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

Meer informatie?

Wil je meer weten over dit thema binnen de watersector bekijk onze webpagina Samenwerking en Expertise (SE). Voor eventuele vragen over dit thema kunt u contact opnemen via cyberweerbaarheidwater@minienw.nl

Samenwerken en Expertise | ⚙ Nieuw of verder te ontwikkelen

Complexiteit instrument
Basis

Bestuurlijk commitment vergroten

De evaluatie van het programma wijst uit dat het bestuurlijk commitment verbeterd kan worden. Met de waterpartners verkennen we de haalbaarheid van het vormen van een 'coalition of the willing' of een ander instrument om meer sponsoring vanuit bestuurders te realiseren. Ook analyseren we of het betrekken van bestaande stuurgroepen bij het programma een toegevoegde waarde hebben voor het commitment en of hier draagvlak voor is.

Bestuurlijke afspraken en gezamenlijke visie en ambitie

We formuleren bestuurlijke afspraken en een gezamenlijke visie en ambitie die als kapstok kan dienen voor het vervolg. Deze werken we uit in SMART-programmadoelen en projectdoel-stellingen om de samenhang te vergroten. Per waterpartner kunnen de doelstellingen verschillen.

Versterken programma-governance

In dit project werken we uit en leggen we vast wat het precieze mandaat en de rol van regiegroep en klankbordgroep binnen het programma zijn. Ook krijgen bestaande gremia waar mogelijk een nadrukkelijkere rol binnen de sectoren. Dit leggen we vast in de programma-governance.

ONE Conference 2023

Voor de ONE Conference van 2023 ontwikkelen we nog nader vast te stellen activiteiten. Om zoveel mogelijk mensen te bereiken werken we samen met andere organisaties.

Borging resultaten programma

Een aanbeveling uit de evaluatie van het programma is om borging en eigenaarschap van resultaten en de verantwoording daarover als vaste taak bij een vaste organisatie te beleggen, zodat de resultaten beschikbaar blijven. Daarnaast is het wenselijk om met capaciteitsbehoud en -uitbreiding te zorgen voor continuïteit en robuustheid van het programmateam. Vanuit dit project doen we een voorstel om hier invulling aan te geven, waarna eventuele besluitvorming kan plaatsvinden.

Complexiteit instrument
Gevorderd

Doorontwikkeling CERT-stelsel watersector

In dit project geven we uitvoering aan de beleidskeuzes gemaakt door IenW over inrichting van het CERT-stelsel in de watersector, in het kader van de implementatie van de NIS2. We maken het CERT-WM sterker en robuuster zodat we voldoen aan de vereisten van CSIRT's die voortvloeien uit NIS2. Daarnaast zal het CERT-WM ook als weerbaarheidscentrum fungeren, in lijn met de functie van Z-CERT in de zorgsector. De ambitie van IenW is om toe te werken naar een CERT Water. Hiertoe ontwikkelen we een businesscase voor de ontwikkeling van een CERT Water, met als doelgroepen waterschappen, Rijkswaterstaat en drinkwater-bedrijven, in nauwe samenwerking met gemeenten (IBD) en provincies. Tot slot geven we inzicht in hoe het doorontwikkelde CERT-stelsel is ingericht en hoe de verschillende CERT's en SOC's met elkaar samenwerken.

Complexiteit instrument
Volwassen

–

Samenwerken en Expertise | ★ Beschikbaar

Complexiteit instrument
Basis

ONE conference water en OT track

Voor het uitwisselen van kennis en expertise zijn tijdens de ONE Conference in 2022 enkele kennissessies georganiseerd. Onder andere is er een OT diner georganiseerd voor deelnemers uit de watersector, is de BIACs gepresenteerd, en zijn de deelnemers meegenomen in red teaming in OT omgevingen. Ook is de serious game cybercrisis een aantal keer gespeeld.

Complexiteit instrument
Gevorderd

Uitbouwen CERT-WM functionaliteit

In 2020 is een analyse uitgevoerd naar de SOC- en CERT-functie binnen RWS en de waterschappen. Er is 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
Volwassen

Center of expertise

In 2022 is 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 is aansluiting gezocht bij de IenW-brede cybersecurity strategie.