

HET CS4NL PROGRAMMA VOOR CYBERSECURITY INNOVATIE



Cybersecurity voor Nederland (CS4NL) geeft een substantiële impuls aan cybersecurity-kennis en -innovatie in Nederland, met rond de 20 miljoen euro subsidie in 2023 alleen al. CS4NL werkt samen met 18 partijen aan een toekomstvisie voor een veiliger Nederland. Deze partijen inspireren elkaar evenals hun achterban en werken samen op overlappende thema's. Concreet resulteert dit in input voor beleid en in subsidieoproepen (calls for proposals), waarbij onderzoeksorganisaties en het bedrijfsleven subsidie aanvragen voor de opzet van een samenwerkingsverband. Partijen schrijven zich in als consortia voor subsidie via NWO (Nederlandse Organisatie voor Wetenschappelijk Onderzoek), via TKI (Topconsortia voor Kennis en Innovatie) en/of voor een SBIR subsidie (Small Business Innovation Research) via het Ministerie van Economische Zaken. Werkt u aan cybersecurity innovaties die bijdragen aan maatschappelijke transitie en de veilige digitale transformaties? Houd dan het CS4NL programma in de gaten en scan de QR code.



Scan mij voor actuele informatie over het CS4NL programma of kijk op www.dcypher.nl > Programmes > CS4NL

ACHTERGROND

Cybersecurity is een belangrijke randvoorwaarde voor een veilige, in rap tempo digitaliserende samenleving. Het belang én de urgentie van cybersecurity voor Nederland blijkt uit de belangrijke plek hiervoor in de Nationale Technologiestrategie evenals het Missie gedreven Topsectoren en Innovatiebeleid (MTIB). Maatschappelijke transitie zijn namelijk vaak afhankelijk van digitalisering en dat kan alleen op een verantwoorde manier als de cybersecurity op orde is. Soms lukt dit met bestaande technologieën, maar soms zijn nieuwe, innovatieve oplossingen nodig. Om middelen van de Rijksoverheid, het bedrijfsleven en kennisinstellingen efficiënt en effectief in te zetten, werken we multidisciplinair en sector overstijgend samen en worden partners zoals lokale overheden betrokken. Veel uitdagingen op het gebied van cybersecurity in verschillende sectoren en de overheid zijn namelijk vergelijkbaar van aard. Het CS4NL programma en de calls zijn vraaggestuurd opgehaald bij de partners en belegd in sector-overstijgende use cases en thema's. Samenwerken gebeurt concreet via calls en kennisdeling vanuit deze calls op de zeven innovatiethema's.

ZEVEN INNOVATIE-THEMA'S

CS4NL werkt vraaggestuurd vanuit de markt. De gedeelde innovatie-thema's zijn:

1. Security by design
2. Veilig datagedreven werken
3. Veilige en robuuste connectiviteit
4. OT/IT-security
5. Cyberrisicomanagement
6. Systeem- en ketenveiligheid
7. Cyber-awareness, kennis en vaardigheden (human capital).



NWO-CALLS

In de calls uitgeschreven door NWO is de **subsidie bedoeld voor interdisciplinair onderzoek door kennisinstellingen (inclusief hogescholen) welke samenwerken met publieke en private partners, inclusief het midden- en kleinbedrijf (MKB)**. Deze projecten gaan over de zeven thema's, hebben een looptijd van maximaal 60 maanden en komen voort uit de KIA (Kennis- en Innovatie Agenda) Sleuteltechnologieën, de KIA Veiligheid en worden ondersteund door het Ministerie van Economische Zaken. Actuele informatie vind je op de [website van NWO](#).

VAN 12 CS4NL USE CASES TOT TKI-CALLS

Een andere mogelijkheid om mee te doen is via TKI (Topconsortia voor Kennis en Innovatie). Deze calls zijn over het algemeen kortcyclisch (max. 3 jaar) en werken via de PPS-innovatieregeling. De TKI-bureaus kiezen in deze calls voor praktische cybersecurity-vraagstukken (de 12 CS4NL use cases), gericht op meerdere toepassingsgebieden, zoals bijvoorbeeld Systeem/Ketenveiligheid en IT/OT security. De 12 CS4NL use cases komen voort uit de zeven innovatie-thema's en de innovatie-behoefte zit bij minimaal 2 topsectoren.

12 USE CASES

- Case 1: Security assessments in complexe systemen
- Case 2: Veilige sensoren voor automatisch inspecteren en detecteren
- Case 3: Cyber Threat Intelligence Sharing and Threat Modelling
- Case 4: Systemisch inzicht in toenemende complexe IT- en OT-systemen
- Case 5: Innovatie op intrusion detection
- Case 6: Supply Chain Security
- Case 7: Supply Chain Security Tool
- Case 8: Systeem- en Ketenweerbaarheid
- Case 9: Modelleren en simuleren van complexe OT/IT-systemen
- Case 10: Veilige apparatuur en applicaties in een thuisomgeving
- Case 11: Veilig datagedreven werken
- Case 12: Cyberweerbaarheid in de logistieke sector

CONCRETE VRAGEN VIA DE SBIR-CALL

Het Ministerie van Economische Zaken werkt samen met het CS4NL programma om SBIR-calls uit te zetten in de CS4NL thema's en use cases. Een SBIR-call is een subsidie-traject waarbij de overheid het MKB uitnodigt tot innovatie voor concrete uitdagingen van de overheid.

Dit start met een haalbaarheidsstudie, daarna een proof of concept demonstratie die de basis kan vormen voor inkoop door de overheid of doorontwikkeling. Een mooie manier voor kleinere bedrijven om een goed idee uit te werken tot tastbaar product en de overheid te laten zien wat ze in huis hebben.

HOE ZIET HET PROCES ERUIT?



CONTACT

www.dcypher.nl (> Programmes > CS4NL)

