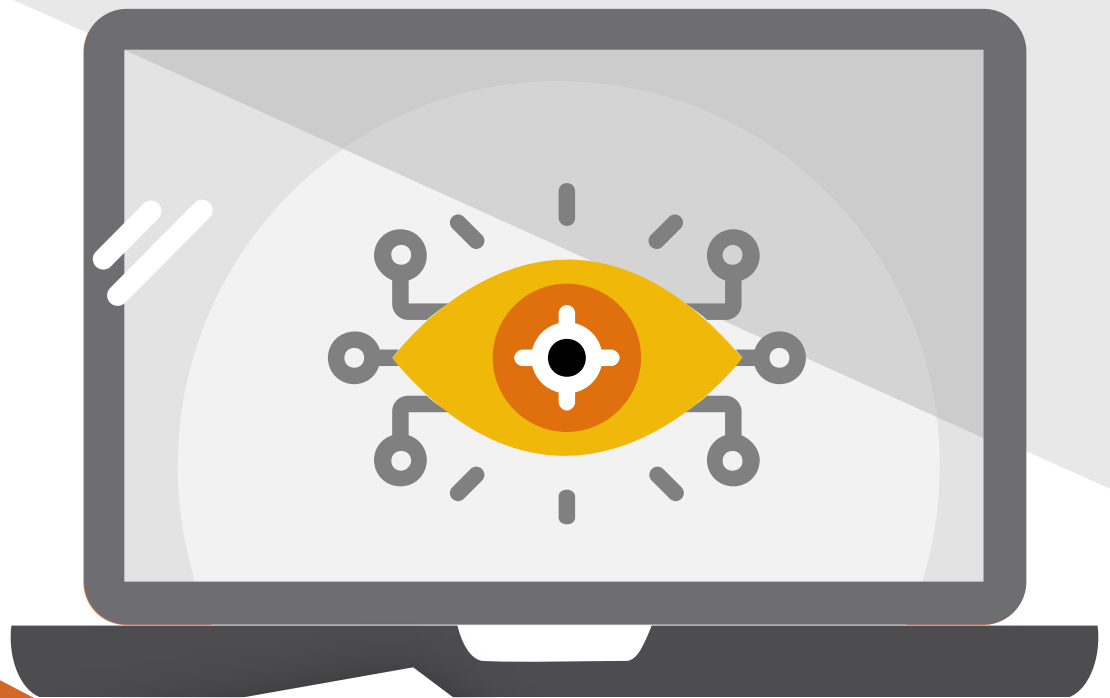


Strategische Agenda 2023 - 2025




CYBERVEILIG
NEDERLAND



Introductie

D Dit document bevat de inhoudelijke agenda voor de periode 2023-2025 met de thema's waar Cyberveilig Nederland in de komende jaren haar activiteiten op wil richten. Deze Strategische Agenda vormt samen met het Strategisch Kader de strategie voor Cyberveilig Nederland. Jaarlijks wordt door de Werkgroep Strategie deze agenda herijkt met als horizon 3 jaar.

In dit document gaan we in op de belangrijkste thema's waar we vanuit Cyberveilig Nederland een bijdrage aan willen leveren. Voor ieder van de thema's beschrijven we de inzet die we vanuit de vereniging beogen. Deze biedt inhoudelijke kaders bij te maken keuzes binnen de verschillende activiteiten die veelal plaatsvinden in projecten en werkgroepen. De activiteiten worden tevens getoetst op de acht eigenschappen die in het strategisch kader zijn uitgewerkt.

Deze eigenschappen zijn:



EIGENSCHAPPEN VAN DE BIJDRAGE VAN DE SECTOR AAN DE MAATSCHAPPIJ

1. **Kwaliteit.** Wat een klant krijgt is voorspelbaar en heeft het beloofde effect.
2. **Transparantie.** Van een product of dienst is duidelijk wat het is, wat het bijdraagt en waarom het in de prijs-range valt waar het valt. Dit helpt potentiële klanten van onze leden om producten en diensten te begrijpen en te vergelijken en zo beter geholpen te worden.



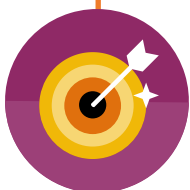
EIGENSCHAPPEN VAN DE RELATIE MET ONZE BELANGHEBBENDEN

3. **Toegankelijkheid.** De vertegenwoordiging van onze sector en dwarsdoorsnedes daarvan is bekend, vindbaar, benaderbaar en inhoudelijk deskundig.
4. **Invloed.** We spannen ons in voor zinvolle security-gerelateerde wet- en regelgeving en voor een gunstig economisch klimaat en werken samen met overheidspartijen als dit de weerbaarheid van de maatschappij ten goede komt. Wij richten ons primair op Nederland maar kunnen ook internationaal activiteiten ontplooiën als dat effectief is.



EIGENSCHAPPEN VAN ONZE LEDEN

5. **Samenwerking.** We delen kennis, tijd en (operationele) informatie om onze gezamenlijke bijdrage (security-effect) te vergroten.
6. **Integriteit.** Integriteit is de basis van al onze activiteiten waarbij wij ons gedragen op een wijze die onze strategie ondersteunt, om ons gezamenlijk effect te vergroten. Wij zijn eerlijk, oprecht en niet omkoopbaar. We zijn transparant, volgen geldende wet- en regelgeving en leggen verantwoording af over ons eigen gedrag en keuzes.



EIGENSCHAPPEN VAN DE VERENIGING

7. **Representatie.** De vereniging vertegenwoordigt een voldoende groot deel van de sector en de samenstelling van het ledenbestand is een representatieve afspiegeling van de sector.
8. **Toekomstbestendigheid.** De vereniging is dusdanig vormgegeven dat ze deze strategie op lange termijn kan blijven uitvoeren.

In de agenda moet telkens worden geborgd dat de activiteiten passen bij tenminste één van deze eigenschappen en met geen van de andere eigenschappen mag botsen. De eigenschappen integriteit (eigenschap 6),

representatie (eigenschap 7) en toekomstbestendigheid (eigenschap 8) hebben geen expliciete koppeling met de strategische agenda en komen daarom niet specifiek terug in de genoemde thema's.



De agenda in vogelvlucht

O Op de agenda voor de komende jaren staan vier thema's waarin we een proactieve benadering kiezen:

A

VERGROTEN KWALITEIT EN TRANSPARANTIE BINNEN DE CYBERSECURITYSECTOR

B

BIJDRAGEN AAN DE ONTWIKKELING VAN BELEID EN STRATEGIE OP GEBIED VAN CYBERSECURITY

C

ONTWIKKELEN VAN EFFECTIEVE PUBLIEK-PRIVATE INFORMATIEDELING IN HET CYBERDOMEIN

D

STEVIGER AGENDEREN VAN OT SECURITY

E Er zijn twee additionele thema's waarin we zoveel mogelijk willen aansluiten op initiatieven van samenwerkingspartners:

E

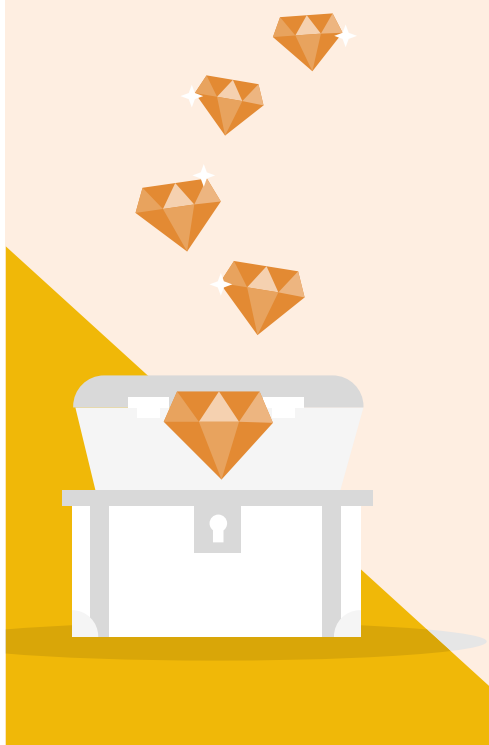
BIJDRAGEN AAN DE ONTWIKKELING VAN MEER HUMAN CAPITAL VOOR DE CYBERSECURITYSECTOR

F

STIMULEREN VAN ONDERZOEK EN INNOVATIE BINNEN HET CYBERSECURITYDOMEIN

A

VERGROTEN KWALITEIT EN TRANSPARANTIE BINNEN DE CYBERSECURITYSECTOR



SLUIT AAN BIJ DE VOLGENDE EIGENSCHAPPEN:

1. Kwaliteit
2. Transparantie
3. Toegankelijkheid

SUBTHEMA'S:

- Ontwikkeling en beheer van certificeringen voor cybersecuritydiensten
 - Zorgen dat ontwikkelde keurmerken in de markt worden uitgevraagd
 - Voor relevante diensten keurmerken ontwikkelen (IR, monitoring, risico, awareness)
Keurmerken laten adopteren op Europees niveau
- Visie neerzetten en uitdragen op wat we als sector zien als basisset aan cybersecuritymaatregelen voor IT én OT (zie ook OT)

B

BIJDRAGEN AAN DE ONTWIKKELING VAN BELEID EN STRATEGIE OP GEBIED VAN CYBERSECURITY

SLUIT AAN BIJ DE VOLGENDE EIGENSCHAPPEN:

3. Toegankelijkheid
4. Invloed

SUBTHEMA'S:

- Overzicht bieden aan leden in het Europese speelveld aan regelgeving
- Zichtbaar beleidsmatige en politieke invloed bereiken op nationaal en Europees niveau op relevante thema's zoals juridische ontwikkelingen (NIS2, CRA, CSA, etc.), ketenveiligheid, etc.
- Bijdrage aan relevante ontwikkelingen vanuit de Cyber Security Raad (CSR) en andere relevante (overleg)gremia



C

ONTWIKKELEN VAN EFFECTIEVE PUBLIEK-PRIVATE INFORMATIEDELING IN HET CYBERDOMEIN



SLUIT AAN BIJ DE VOLGENDE EIGENSCHAPPEN:

3. Toegankelijkheid
5. Samenwerking

SUBTHEMA'S:

- Stimuleren van informatie-uitwisseling vanuit de leden van CVNL in de Nederlandse aanpak van ransomwarebestrijding (doorontwikkelen project Melissa)
- Stimuleren van informatie-uitwisseling vanuit de leden van CVNL in belangrijke overheidsprogramma's en samenwerkingen rondom informatiedeling, zoals Programma Cyclotron

D

STEVIGER AGENDEREN VAN OT-SECURITY

SLUIT AAN BIJ DE VOLGENDE EIGENSCHAPPEN:

1. Kwaliteit
2. Transparantie
3. Toegankelijkheid

SUBTHEMA'S:

- Zichtbare rol CVNL-leden in de IACS-coalitie
- Ontwikkelen van kwaliteitsregelingen voor bevordering OT-security
- Visie neerzetten en uitdragen op wat we als sector zien als basisset aan cybersecuritymaatregelen voor OT (zie ook Kwaliteit en Transparantie)



E

BIJDRAGEN AAN DE ONTWIKKELING VAN MEER HUMAN CAPITAL VOOR DE CYBERSECURITYSECTOR



EIGENSCHAPPEN:

3. Toegankelijkheid
5. Samenwerken

SUBTHEMA'S:

- Aansluiten bij initiatieven die bijdragen aan de ontwikkeling van meer human capital voor de cybersecuritysector

F

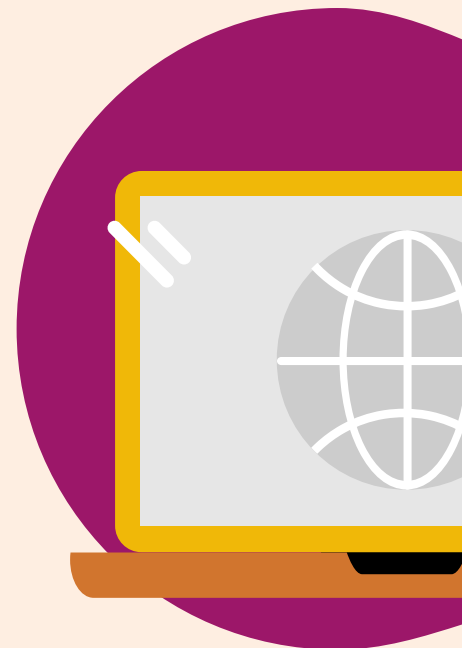
STIMULEREN VAN ONDERZOEK EN INNOVATIE BINNEN HET CYBERSECURITYDOMEIN

EIGENSCHAPPEN:

3. Toegankelijkheid
5. Samenwerken

SUBTHEMA'S:

- Verbinden van de cybersecuritysector aan initiatieven op gebied van (wetenschappelijk) onderzoek en innovatie



Colofon

Dit is een uitgave van Cyberveilig Nederland. De inhoud van deze uitgave is met grote zorg samengesteld. Toch kan er onverhoopt een fout of onvolledigheid in zijn geslopen. Cyberveilig Nederland kan daarvoor niet aansprakelijk worden gesteld.

Dit Strategisch Kader is mede tot stand gekomen met input van de leden van Cyberveilig Nederland en vertegenwoordigers van het NCSC, DTC, Accss, DIVD, NLDigital, dcypher en DINL

Meer informatie over de activiteiten van Cyberveilig Nederland vindt u op cyberveilignederland.nl

Contactgegevens

E-mail: info@cyberveilignederland.nl

Telefoon: **088 - 118 25 10**

