PARTNERDECK

PROJECT ENERGIE

Inhoud

Over DIVD

De beschermers van de digitale wereld

Vijf jaar geleden richtte een groep enthousiaste ethische hackers het Dutch Institute of Vulnerability Disclosure (DIVD) op, met als doel de digitale wereld veiliger te maken. Vandaag de dag is ons team gegroeid tot bijna 200 toegewijde en vaardige professionals die samen werken aan dezelfde missie.

DIVD helpt het internet veiliger te maken door kwetsbaarheden in systemen op te sporen en de eigenaren hiervan op de hoogte te stellen. Als we een onbekende kwetsbaarheid (een zero-day) vinden, melden we dit aan leveranciers zodat het opgelost kan worden voordat het wordt misbruikt. Daarnaast notificeren we eigenaren van kwetsbare ip-adressen met informatie over een update of patch.

Onze missie
Wij zoeken naar online kwetsbaarheden en melden die bij degenen die ze kunnen verhelpen. We doen dat wereldwijd, maar wel op z’n Nederlands: open, eerlijk, direct en gratis.

Dit is wat wij doen

Wij onderzoeken kwetsbaarheden

Wij zoeken naar **bekende kwetsbaarheden**, ook wel CVE's: Common Vulnerabilities and Exposures. Dit zijn kwetsbaarheden in systemen die openbaar bekend zijn en gebruikt kunnen worden om websites, databases of apparaten te hacken. Als we een kwetsbaarheid vinden, melden we die bij de eigenaar van het systeem, met een mogelijke oplossing.

Wij vinden zero-days

Naast het onderzoeken van bekende kwetsbaarheden, zoeken we ook naar nieuwe, **onbekende kwetsbaarheden**, zero-days. Deze zijn onbekend voor anderen en hebben vaak nog geen oplossing of patch en vormen daardoor een extra risico. Vervolgens melden wij deze zero-day aan de (software) leverancier zodat die het probleem kunnen verhelpen en een update kunnen uitbrengen.

Wij waarschuwen betrokkenen

Na het onderzoeken van kwetsbaarheden brengen we kwetsbare systemen in kaart d.m.v. het scannen op ip-adressen. Vervolgens **sturen we een notificatie** naar de eigenaar met informatie over update of patch. Bij gestolen of openbaar gemaakte gegevens waarschuwen we betrokkenen en adviseren we hen passende maatregelen te nemen, bijvoorbeeld het wijzigen van je wachtwoord.

CVE

Wij zijn een CVE Numbering Authority (CNA)
CVE staat voor: Common Vulnerabilities and Exposures. We identificeren kwetsbaarheden en geven ze unieke identificatienummers (CVEs). Daarnaast helpen we onderzoekers om kwetsbaarheden op een verantwoorde manier aan leveranciers bekend te maken..

Ethisch Hacken

Hacken binnen de wet

Bedrijven en de overheid mogen dergelijke acties alleen doen met geïnformeerde toestemming. Wij, als vrijwilligersorganisatie, zijn niet gebonden aan deze verplichting om vooraf te informeren.

De Nederlandse rechtspraak staat ons toe kwetsbaarheden te onderzoeken om misbruik te voorkomen, mits we handelen in een wezenlijk maatschappelijk belang, proportioneel te werk gaan en er geen minder ingrijpende alternatieven beschikbaar zijn. Dankzij ons vrijwillige karakter en het naleven van deze strikte voorwaarden is onze werkwijze goedgekeurd door het Openbaar Ministerie, het Nationaal Cyber Security Centrum en andere autoriteiten.

De Onderzoeksraad voor Veiligheid concludeerde in diens evaluatie van o.a onze Citrix-case dat digitale veiligheid grotendeels afhankelijk is van vrijwilligers zoals wij. Bovendien benadrukte de Nederlandse Minister van Justitie tijdens een parlementaire discussie dat DIVD een essentiële rol vervult in het beveiligen van het internet, omdat wij dit mogen doen terwijl de overheid daartoe niet bevoegd is.

We hebben een gedragscode (Code of Conduct) opgesteld die de ethische basis vormt voor ons werk. **divd.nl/code**

“DIVD doet echt buitengewoon goed werk en daar zijn we heel blij mee. Het NCSC werkt waar mogelijk met hen samen en zal dat blijven doen.”

Dilan Yeşilgöz,
MINISTER VAN JUSTITIE EN VEILIGHEID

DIVD in cijfers

1.336.617
Kwetsbare IPS gemeld

85
CVE’s toegewezen

163
Totaal cases

189
Aantal leden

32
Huidig aantal partners

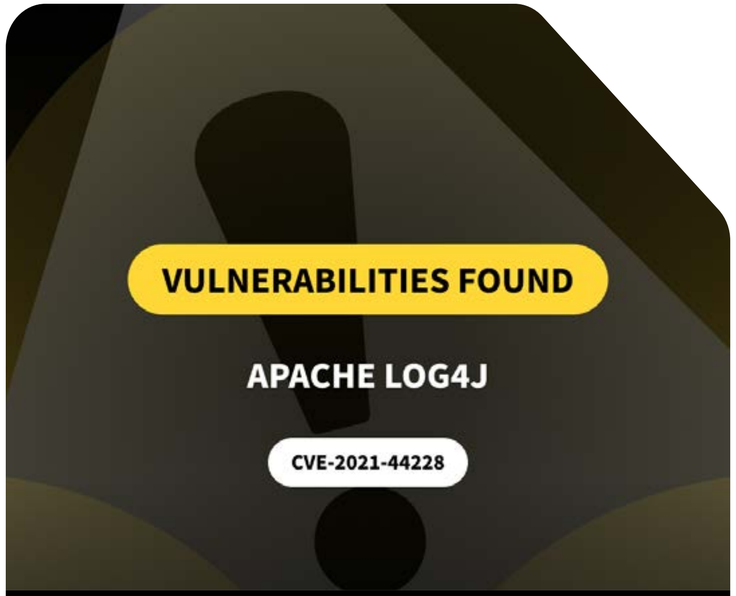
1.223.000.486
Beoordeelde inloggegevens

Hier zijn we trots op

Operation Endgame

Met deze internationale samenwerking waarbij diverse botnets zijn uitgeschakeld, hebben wij de 16 miljoen slachtoffers over hen gelekte credentails genotificeerd.

LEES MEER



Log4j

Er werden kwetsbaarheden in Log4J gevonden waardoor remode code execution mogelijk was. Samen met NCSC hebben we slachtoffers genotificeerd.

LEES MEER

Citrix

Deze kwetsbaarheden zorgde ervoor dat cybercriminelen toegang konden krijgen tot systemen, dit was onze eerste grote case met wereldwijde impact en media aandacht.

LEES MEER

Dit zijn wij

DIVD bestaat uit vrijwillgers, medewerkers en partners.

Met bijna 200 vrijwilligers werken we aan onze missie om het internet veiliger te maken door kwetsbaarheden op te sporen en slachtoffers te waarschuwen. We doen dit met een team van experts, ethische hackers en onderzoekers die samenwerken om dreigingen te identificeren en mitigeren, idealiter voordat ze misbruikt worden.

Sinds onze oprichting in 2019 hebben we duizenden organisaties en miljoenen burgers wereldwijd gewaarschuwd voor kwetsbaarheden in hun systemen, waardoor we mogelijk grote datalekken en cyberaanvallen hebben voorkomen. Onze onderoeken leiden tot Kamervragen, beleidswijzigingen en een verbeterde digitale weerbaarheid binnen diverse sectoren. We geloven in samenwerken en community, daarom werken we samen met overheden, bedrijven en internationale partners.

Wij geloven in de kracht van samenwerking. Daarom werken we nauw samen met overheden, bedrijven en internationale partners.

Foto van partners en vrijwilligers op onze jaarlijkse partnerdag in 2024.

Deze organisaties supporten onze missie

PROJECT ENERGIE

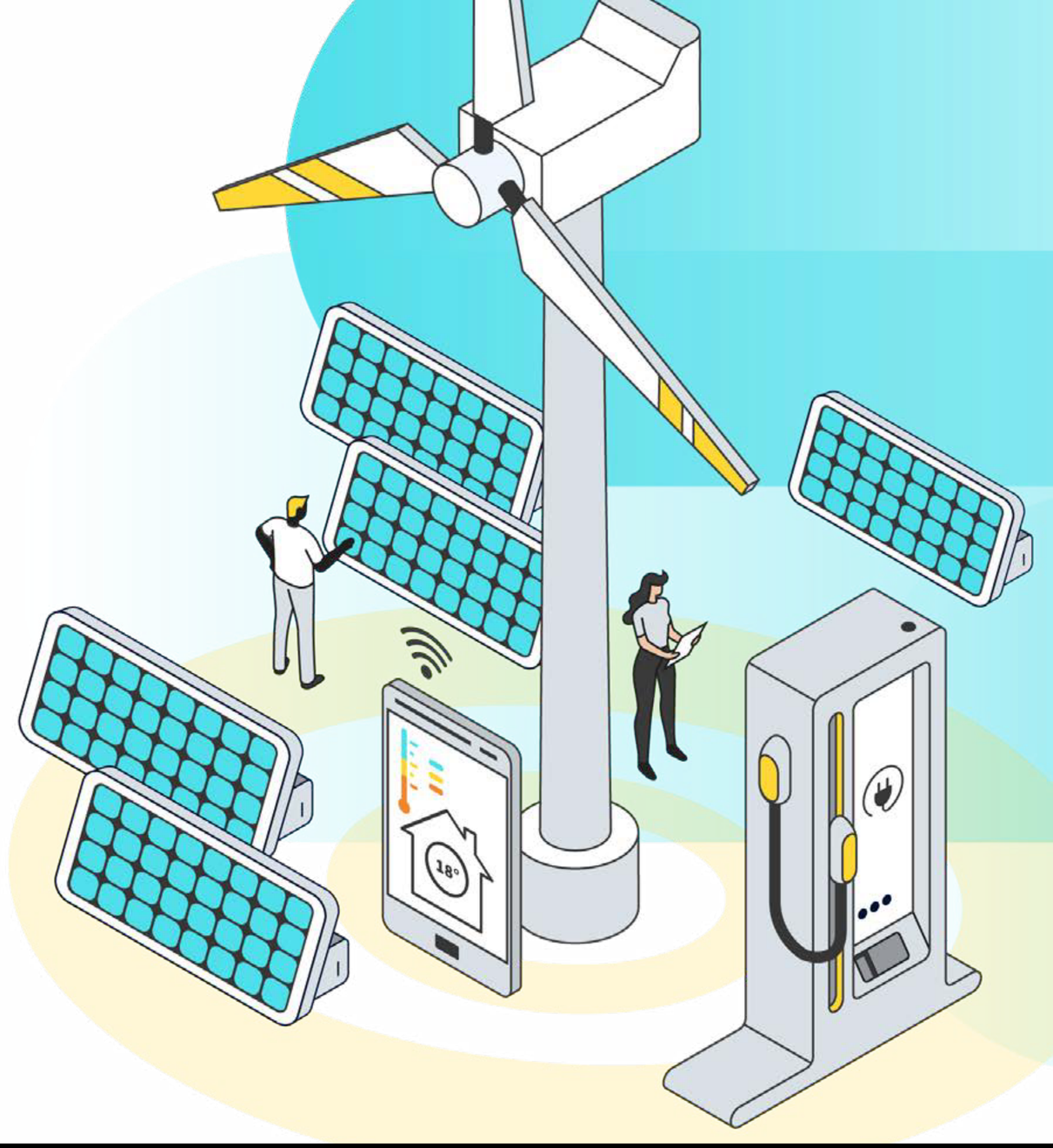
Coordinated Vulnerability Disclosure (CVD)
in de energiesector.

Een slimme, duurzame, maar kwetsbare energiesector:

waarom veiligheid cruciaal is.

Het Europese elektriciteitsnetwerk is een ‘smart grid’ geworden, waarin consumenten zowel gebruikers als producenten van energie zijn. Slimme, online verbonden apparaten helpen vraag en aanbod beter op elkaar af te stemmen, wat kansen biedt voor verduurzaming en marktinnovatie. Tegelijkertijd maakt dit ons energiesysteem kwetsbaar voor digitale aanvallen, zoals het bedreigende ‘Black-Out scenario, waarin cybercriminelen slimme apparaten manipuleren en grootschalige stroomstoringen veroorzaken.

Met het project CVD in het Energiesysteem gaat DIVD samen met partners in de energiesector kwetsbaarheden opsporen en aanpakken. We onderzoeken niet alleen randapparatuur zoals laadpalen en zonnepanelen, maar ook de apps en online platforms waarmee deze apparaten worden aangestuurd. Daarnaast bouwen we een hardwarelab voor diepgaand onderzoek en leiden we nieuwe experts op via de DIVD.academy.



Het Black-Out scenario

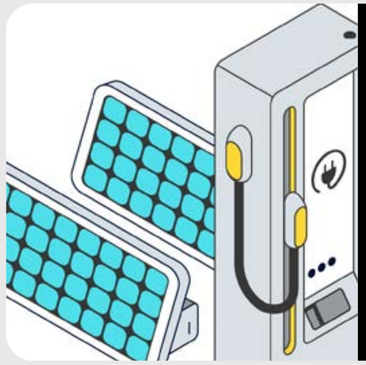
De grootste dreiging voor de energiesector is een Black-Out scenario, waarbij cybercriminelen erin slagen om het elektriciteitsnet ernstig te verstoren. Dit kan gebeuren door een grootschalige cyberaanval waarbij slimme energieapparaten, zoals bijvoorbeeld zonnepanelen, laadpalen, slimme meters en windmolens, op afstand worden gemanipuleerd. In een gecoördineerde aanval kunnen deze apparaten plotseling worden uitgeschakeld of juist massaal worden ingeschakeld, wat het elektriciteitsnet ernstig uit balans brengt.

Netbeheerders spelen een cruciale rol in het in balans houden van het elektriciteitsnet en reageren snel op schommelingen in vraag en aanbod. Wanneer echter grote hoeveelheden energie in korte tijd worden ingevoerd of afgenomen, kan dit de stabiliteit van het net onder druk zetten. Dit kan leiden tot regionale stroomuitval, die in een domino-effect kan overslaan naar nationale of zelfs continentale black-outs. De gevolgen hiervan zijn enorm: essentiële infrastructuren zoals communicatie, transport, gezondheidszorg en betalingsverkeer kunnen stilvallen, met mogelijk desastreuze gevolgen voor de samenleving en economische schade ter waarde van miljarden euro’s.

Een Black-Out scenario is geen theoretische dreiging, maar een reëel risico dat vraagt om doordachte preventie en digitale weerbaarheid binnen de energiesector.

Wat gaan we precies doen?

Met het project CVD in de energiesector starten we een nieuwe onderzoekslijn om de digitale weerbaarheid van het steeds kwetsbaarder wordende energiesysteem te versterken. We richten ons op kennisontwikkeling, samenwerking en bewustwording binnen de sector en onderzoeken daarbij specifiek kwetsbaarheden in randapparatuur, zoals laadpalen, omvormers, thuisbatterijen en energiebeheersystemen. Eerdere bevindingen leidden al tot Kamervragen en acties van autoriteiten zoals de Rijksinspectie Digitale Infrastructuur (RDI).
In 2025 zetten we hierin de volgende stappen:



IoT Hacking Lab

We zetten een IoT Hacking Lab op om onder andere randapparatuur zoals laadpalen, thuisbatterijen, omvormers e.d. te onderzoeken en testen. Daarnaast werken we samen met andere labs.

Onderzoek

We doen en publiceren onderzoek om hiermee autoriteiten en partners te ondersteunen bij handhaving en het implementeren van verbeteringen binnen de energiesector.

Educatie

We leiden nieuwe experts op met **DIVD. Academy** door lesmateriaal, trainingen en workshops te ontwikkelen voor studenten, de installatiebranche en onderwijsinstellingen in de energiesector.

Samenwerken

We werken samen met netbeheerders, overheden, leveranciers, fabrikanten, etc. om bewustzijn binnen de sector te vergroten en kwetsbaarheden te vinden en op te lossen.

Zo kun je helpen

Financiën

Hoewel DIVD wordt gerund door bijna 200 Nederlandse vrijwilligers, hebben we financiële middelen nodig om ons werk effectief te blijven doen. Om continuïteit te waarborgen en te groeien, hebben we een stabiele financiering van minimaal €200.000 per jaar nodig. Dit stelt ons in staat te investeren in professionele ondersteuning, essentiële diensten, tools en medewerkers.

We zijn hierbij volledig afhankelijk van sponsoren en donateurs. Daarom zoeken we organisaties en individuen die ons willen steunen met terugkerende jaarlijkse donaties vanaf €5.000 per jaar.

Direct doneren, ga naar: **divd.nl/donate**

Materialen

Onze organisatie is sterk afhankelijk van IT. Gelukkig krijgen we al veel steun van leveranciers in de vorm van gratis licenties, tools en diensten.
Hoewel we geen productaanbevelingen doen – om onze ANBI-status en onafhankelijkheid te waarborgen – erkennen we graag een bijdrage op onze partnerpagina.

Daarnaast ondersteunen veel partners ons niet alleen op IT-gebied, maar ook met juridische, communicatieve en organisatorische expertise.

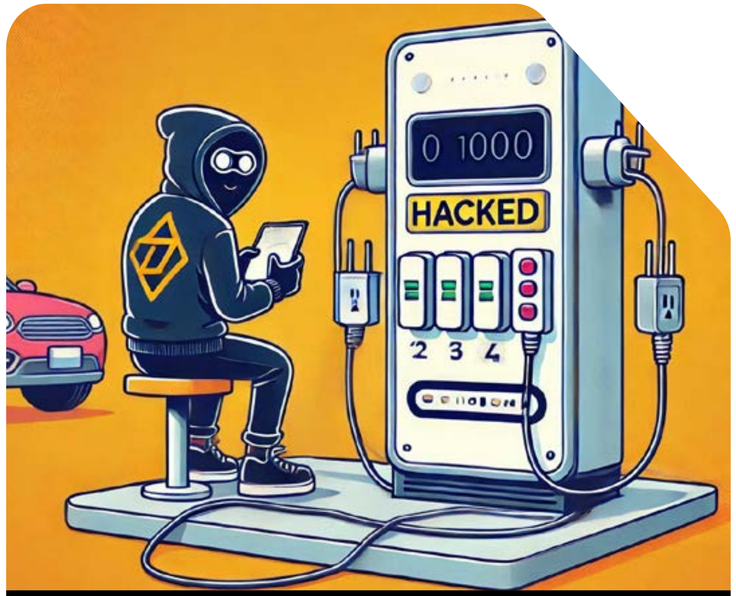
Mensen

Organisaties kunnen ons ondersteunen met de meest waardevolle hulpbron: mensen. Door medewerkers structureel een aantal uur per week de ruimte te geven om zich voor een langere periode in te zetten als vrijwilliger bij DIVD, dragen zij direct bij aan onze missie.

Dit draagt niet alleen bij aan hun persoonlijke ontwikkeling, maar laat ook zien dat hun werkgever onze missie ondersteunt en actief invulling geeft aan maatschappelijk verantwoord ondernemen.

Security researchers binnen de energiesector zijn meer dan welkom om zich als vrijwilliger bij DIVD aan te sluiten.

Onze eerdere energiesector onderzoeken



ioCharger

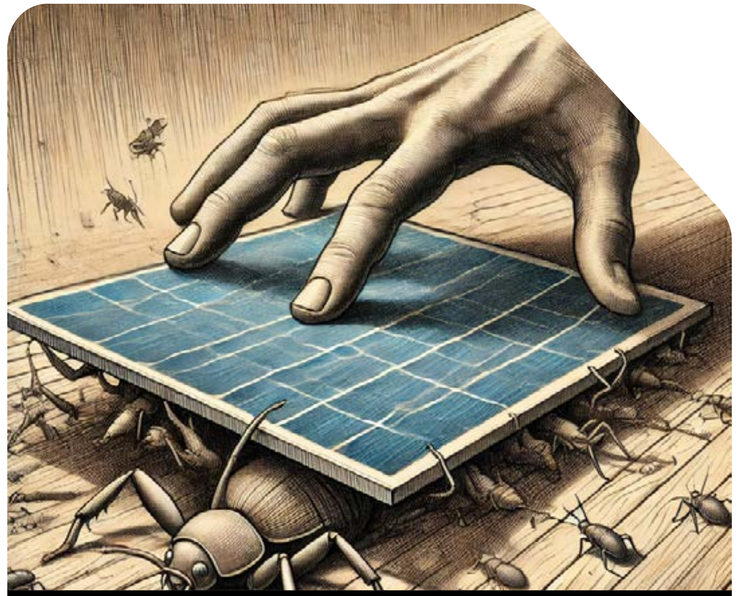
In ons onderzoek naar de beveiliging van EV-laders zijn 17 nieuwe kwetsbaarheden (zero-days) ontdekt in laders van iocharger.

LEES MEER

Solarman

We vonden de super admin gegevens op Github, waardoor we toegang kregen tot bijna 1 miljoen installaties wereldwijd.

LEES MEER



Enphase

We ontdekten zes zero-day kwetsbaarheden in de omvormers, waarmee we wereldwijd 6 miljoen omvormers over konden nemen.

LEES MEER

Deze organisaties supporten ons energieproject

FINANCE

SIDN Fonds

SIDN investeert in projecten met lef en maatschappelijke meerwaarde, die bijdragen aan een sterk internet, sterke internetgebruikers of die zich richten op de publieke waarden en maatschappelijke kant van het internet.

GA NAAR SITE

FINANCE

Topsector Energie

Topsector Energie helpt bedrijven, kennisinstellingen, overheden en maatschappelijke organisaties samen te werken aan het energiesysteem van de toekomst.

GA NAAR SITE

Neem contact op

Wil je meer weten over DIVD, het werk wat we doen, de impact die we maken of wil je gewoon partner worden? Twijfel niet en neem contact op met onze managing director.

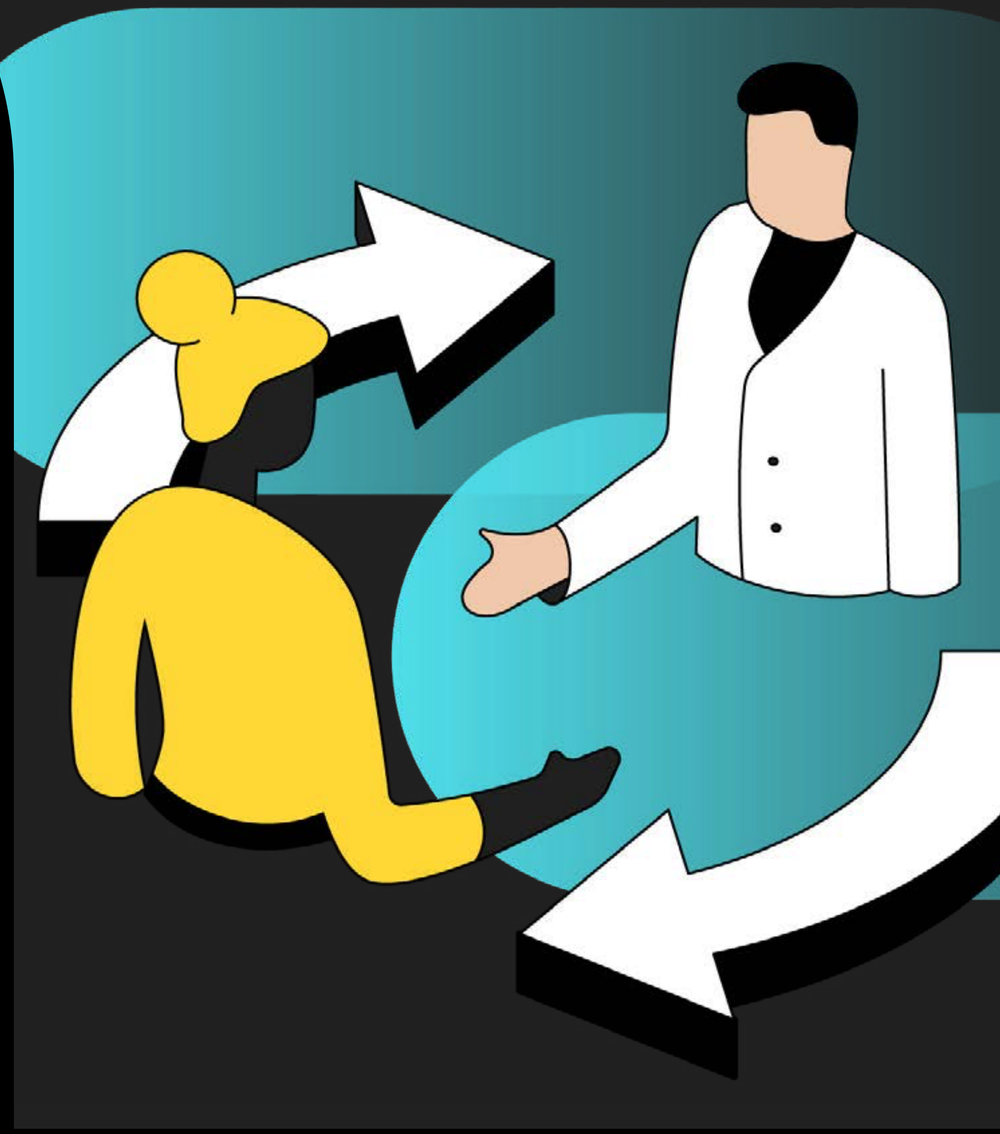
Chris van't Hof
Managing Director DIVD

partners@divd.nl

Chris van 't hof

(+31) 70 41 90 309

Maanweg 174
2516 AB Den Haag



Dutch Institute for Vulnerability Disclosure