Richard van Hooijdonk

KEYNOTE OVER AI, CYBERCRIME EN WEERBAARHEID

Cybercrime in het AI-tijdperk

Criminelen gebruiken AI om sneller, op grotere schaal en overtuigender toe te slaan. Deze keynote laat zien wat ze nu doen, wat er de komende jaren aankomt en hoe een weerbare organisatie AI in haar voordeel inzet.

In deze keynote laat hij zien hoe criminelen AI gebruiken, van gekloonde stemmen en nepwebshops tot AI-agents die zelf naar zwakke plekken zoeken, waar criminaliteit de komende jaren naartoe gaat en hoe organisaties zich daartegen wapenen. Hij sprak hierover voor politie, defensie en internationale politiesamenwerking.

RICHARD VAN HOOIJDONK

Richard van Hooijdonk is trendwatcher, futurist en internationaal keynotespreker. Veel trendwatchers en futuristen bekijken de toekomst van een afstand. Richard van Hooijdonk leeft erin. Zijn team bestaat uit mensen en AI-agents en hij heeft meerdere chips geïmplanteerd in zijn lichaam. Hij spreekt over AI en nieuwe technologie, over de organisatie van de toekomst en over leiderschap in tijden van AI. Hij neemt je mee naar een toekomst die je je nu nauwelijks kunt voorstellen, en laat zien hoe je er zelf richting aan geeft.

3.000+	650.000+	30+	Bestseller
keynotes	deelnemers	landen	auteur

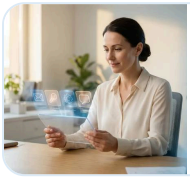
De keynote in 22 onderwerpen

Als aanvallen steeds slimmer en sneller worden, moet de verdediging mee veranderen. AI maakt cybercrime een vraagstuk voor de hele organisatie.

DE DREIGING

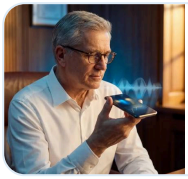
Hoe criminelen AI gebruiken

Wat AI verandert aan phishing, fraude, afpersing en inbraken, en aan de manier waarop criminelen zich organiseren.



01 Crime-as-a-service

Criminelen huren al jaren gereedschap en kennis in. AI vergroot dat aanbod: overtuigende phishing in vele talen en modellen zonder remmen.



02 Deepfakes en stemklonen

Een nagebootste stem of video van een bestuurder of familielid. Echt en nagemaakt zijn steeds lastiger uit elkaar te houden.

03 Fraude op industriële schaal

Synthetische identiteiten, nepwebshops en beleggingsfraude waarbij chatbots helpen om veel slachtoffers tegelijk te bespelen.

04 AI die zwakke plekken vindt

AI leest code, tast systemen af en vindt lekken die jarenlang onopgemerkt bleven. Ook criminelen experimenteren met deze techniek.

05 Gijzelsoftware als verdienmodel

Criminele groepen werken als bedrijven, met AI voor verkenning, onderhandeling en afpersing met gestolen gegevens.

06 De nepsollicitant

Een kandidaat met een verzonnen cv, een gestolen identiteit en soms een AI-gezicht solliciteert op afstand. Eenmaal aangenomen heeft hij de sleutels.

07 Aanvallen op AI zelf

Verborgen opdrachten, vergiftigde trainingsdata en gestolen modellen. De AI van de organisatie is zelf een doelwit.

08 Nepnieuws als wapen

Een nepverklaring van een topbestuurder of een nagemaakte rampfoto: desinformatie met AI kan beurskoersen bewegen en reputaties beschadigen.

09 Inbraak via de keten

Eén besmette update of softwarebouwsteen kan duizenden klanten tegelijk raken. AI helpt aanvallers een ingang in de keten te vinden.

DE TOEKOMST

De toekomst van criminaliteit

Waar criminaliteit over vijf tot vijftien jaar kan staan: aanvallen die zichzelf uitvoeren, versleuteling die breekt en misdaad die uit het scherm stapt.

10 De aanval die zichzelf uitvoert

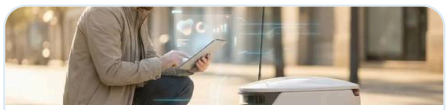
BEGINT NU

De eerste aanvallen waarin AI het meeste werk doet, zijn gemeld. Straks verkennen, inbreken en onderhandelen agents bij duizenden doelwitten tegelijk.

11 Als versleuteling breekt

TOEKOMSTSCENARIO

Een toekomstige quantumcomputer kan veelgebruikte versleuteling breken. Criminelen en staten verzamelen versleutelde gegevens alvast.



12 Misdaad stapt uit het scherm

TOEKOMSTSCENARIO

Robots, drones en zelfrijdende auto's gaan samenwerken en hun werk zelf plannen. Wie hun aansturing hackt, kan de straat en het magazijn raken.

DUUR
30, 45, 60 minuten of langer, met ruimte voor vragen

TAAL
Nederlands of Engels

VORM
Op locatie of online

KOSTEN
Op aanvraag

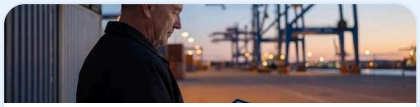
DE ANDERE KANT

Kritieke infrastructuur

Waarom stroom, water, zorg en havens kwetsbaar zijn, waar misdaad en conflict elkaar raken en hoeveel toezicht een veilige samenleving wil.

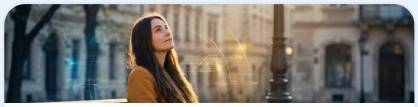
13 Kritieke infrastructuur als prooi

Energie, water, ziekenhuizen, havens en netwerken draaien deels op oude besturing die nu online is, en dus op afstand bereikbaar.



14 Criminelen in dienst van staten

Sommige overheden laten criminele groepen inbreken, saboteren en spioneren. Voor het slachtoffer lijkt het gewone cybercrime.



15 Veilig en vrij

AI kan netwerkverkeer en gedrag van mensen steeds nauwkeuriger volgen. Daarmee wordt de grens tussen veiligheid en toezicht een keuze.

DE ORGANISATIE

De weerbare organisatie

Hoe een organisatie zich wapent tegen criminelen met AI: mens en AI in één team, nieuwe rollen, een bestuur dat richting geeft en partners over de hele wereld.

16 De AI-first organisatie

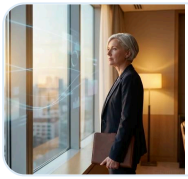
In cyberveiligheid doet AI het herhalende en voorspellende werk, en ontdekt het dreigingen sneller dan mensen ooit kunnen. Het team oordeelt en kiest.

17 Verdedigen met AI

AI ziet afwijkend gedrag in netwerken, gestolen accounts en misbruikte leveranciersrechten, en kan binnen seconden ingrijpen.

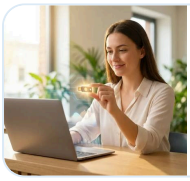
18 Nieuwe rollen in de beveiliging

Specialisten die de eigen AI aanvallen om die te testen, mensen die toezicht houden op verdedigende agents, en analisten die met AI werken.



19 Weerbaarheid als bestuurstaak

Regels maken bestuurders verantwoordelijk voor digitale veiligheid. Zij beslissen ook wat AI zelf mag doen.



20 De mens als eerste verdediging

Veel aanvallen beginnen bij een mens. In een cultuur waarin melden normaal is, wordt elke medewerker een sensor.

21 De toekomstacademie

Echte incidenten worden lesstof in een toekomstacademie, waar ervaren medewerkers en nieuwkomers geregeld oefenen met AI en nieuwe technologie.

22 Samen sterker dan de crimineel

Criminelen werken wereldwijd samen. Verdedigers ook: in internationale ecosystemen van bedrijven, onderzoekers, politie en overheden.

PLUS

"Het is Richard uitstekend gelukt om onze leiders wakker te schudden en hen op het spoor van de toekomst te zetten: er is na de lezing op verschillende plaatsen in de organisatie nagepraat over de onderwerpen en er zijn initiatieven in gang gezet."

Aart van Haren Algemeen directeur, PLUS

Deloitte.

"Een flitsende reis langs nieuwe technologie. Zijn enthousiaste en energieke manier van presenteren en visuele ondersteuning ervan zorgden voor een geslaagde aftrap van het event."

Patrick Steemers Partner, Deloitte

Interesse in Cybercrime in het AI-tijdperk voor je evenement?

E-MAIL
talks@vanhooijdonk.com

TELEFOON
085 303 0792

SITE
richardvanhooijdonk.com