NL
SECURE
[ID] LET'S TALK ABOUT IT
2025

HÉT SECURITY-EVENT VAN NEDERLAND

PROGRAMMA
NLSECURE[ID]
2025

BELANGRIJKE INFORMATIE

LOCATIE
NBC Congrescentrum Nieuwegein

TIJD
10.00 – 17.30 uur

AANMELDEN
kpn.com/nlsecure

kpn

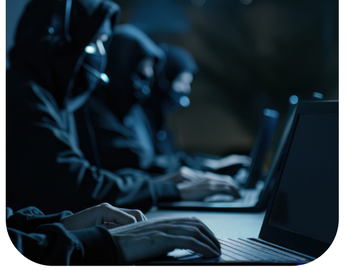
PROGRAMMA
NLSECURE[ID]
2025

NLSECURE[ID]

Kennisdeling is essentieel voor het vergroten van de digitale weerbaarheid van Nederland. Daarom organiseert KPN op 21 januari voor de 9e keer NLSecure[ID], hét event voor de Nederlandse securitycommunity.

Tijdens dit jaarlijkse event krijg je de laatste inzichten in relevante security- en marktontwikkelingen. Experts delen hun kennis en ervaring, waarmee jij je security naar een hoger niveau tilt. Het motto van NLSecure[ID] is dan ook: 'Security, let's talk about it!'.

PROGRAMMA NLSECURE[ID] 2025



THEMA 2025

'LET'S TALK ABOUT... THE FUTURE OF CYBER'

Het thema van deze editie is 'Let's talk about... the Future of Cyber'. De digitale wereld verandert snel en cyberbedreigingen raken niet alleen technologie, maar doordringen in elke laag van onze samenleving. Het gaat niet alleen om up-to-date blijven, maar ook om het aanpakken van nieuwe vraagstukken. Wie neemt de leiding als de grenzen tussen digitaal en fysiek vervagen? Het antwoord ligt in een verschuiving binnen het vakgebied zelf: verantwoordelijkheid herdefiniëren, nieuwe modellen omarmen en de securitycommunity versterken. Alleen zo kunnen we ons voorbereiden op de dreigingen van de toekomst.

PROGRAMMA
NLSECURE[ID]
2025

PROGRAMMA

10.00 - 11.00	ONTVANGST
11.00 - 12.30	OPENING & KEYNOTES
12.30 - 13.30	NETWERKLUNCH
13.30 - 14.15	TALKS RONDE 1
14.15 - 15.00	TALKS RONDE 2
15.00 - 15.45	PAUZE
15.45 - 16.30	TALKS RONDE 3
16.30 - 17.30	NETWERKBORREL

kpn

PROGRAMMA NLSECURE[ID] 2025

KEYNOTES

CHANTAL VERGOUW

CHIEF BUSINESS MARKET,
LID RAAD VAN BESTUUR
KPN

Van zelfredzaamheid naar collectieve veerkracht

Cyberdreigingen groeien exponentieel, en met de komst van nieuwe technologieën, zoals AI en Quantum computing, zal dit alleen maar versnellen. Om deze dreigingen aan te pakken, moeten we als samenleving gezamenlijk verantwoordelijkheid nemen en elkaar ondersteunen in de bescherming van de digitale keten. Alleen door intensieve samenwerking en het delen van kennis en expertise kunnen we als securitycommunity sterker worden en de continuïteit waarborgen. Chantal roept op tot een verschuiving van zelfredzaamheid naar collectieve veerkracht, waarbij we elkaar ondersteunen en versterken om de veiligheid van onze samenleving te garanderen.

PROGRAMMA NLSECURE[ID] 2025

KEYNOTES

MEINDERT KAMPHUIS

HEAD AI SAFETY & SECURITY LAB
RIJKSINSPECTIE DIGITALE INFRASTRUCTUUR

Waarom de RDI samen met de AIVD AI-initiatieven aanjaagt

Tijdens ditzelfde event vorig jaar benadrukte de AIVD de noodzaak van een fundamentele cultuurverandering. De toenemende complexiteit van digitale dreigingen vraagt om een nieuwe aanpak en intensievere samenwerking. Ook de RDI herkent deze urgentie. Hoewel een toezichthouder van nature terughoudend is, werd duidelijk dat gezamenlijke actie op het gebied van AI onvermijdelijk was. Zo werd AI36 opgericht: een initiatief waarin de RDI en de AIVD hun krachten bundelen om AI-gedreven oplossingen te ontwikkelen voor de veiligheid en weerbaarheid van onze digitale samenleving. Meindert legt in zijn talk uit hoe deze samenwerking bijdraagt aan nationale veiligheid en digitale weerbaarheid.

PROGRAMMA NLSECURE[ID] 2025

KEYNOTES

TOM-MARTIJN ROELOFS

GLOBAL HEAD OF SECURITY STRATEGY AND DATA
ING

The Future of Cyber: hoe ING AI inzet voor toekomstbestendige security

Tom-Martijn zal uitgebreid toelichten hoe ING kunstmatige intelligentie (AI) inzet om de beveiliging voortdurend te versterken en toekomstbestendig te maken. Hij biedt een diepgaand inzicht vanuit zowel een organisatorisch als technologisch perspectief en bespreekt de innovaties die ING heeft doorgevoerd om AI in te zetten voor het detecteren van bedreigingen, het verbeteren van reactietijden en het versterken van de algehele beveiligingsinfrastructuur. Tom-Martijn zal concrete use cases presenteren die als inspiratie kunnen dienen voor andere organisaties die hun eigen cyberbeveiliging willen verbeteren.

KEYNOTES

EPPO VAN NISPEN TOT SEVENAER

CEO
NEDERLANDS INSTITUUT VOOR BEELD EN GELUID

De digitalisering van Nederland: een terug- en vooruitblik

Tijdens het event neemt Eppo je mee op een visuele reis door de digitalisering van Nederland. Met behulp van spraakmakende tv-fragmenten en ander uniek beeldmateriaal vertelt hij het verhaal van de technologische veranderingen die ons leven hebben vormgegeven. Van de eerste computers en mobiele telefoons tot de razendsnelle opkomst van kunstmatige intelligentie en de steeds grotere rol van cybersecurity in onze samenleving. Deze sessie biedt een reflectie op de indrukwekkende vooruitgangen van de afgelopen decennia, maar vraagt ook aandacht voor de grote uitdagingen die voor ons liggen. Waar blijft de mens in deze snel evoluerende digitale wereld?

PROGRAMMA
NLSECURE[ID]
2025

VOLGENDE TALK »

GREEN TALKS

RAFFAELE MARESCA

GLOBAL CHIEF INFORMATION SECURITY OFFICER
AKZONOBEL

Cybersecurity: voorbij de steeds veranderende digitale risico's
In een wereld waarin digitale technologieën een steeds centralere rol spelen, staan organisaties continu voor nieuwe cyberdreigingen. Ondanks aanzienlijke investeringen in security blijven de risico's toenemen en complexer worden. Raffaele neemt je mee door de evolutie van cyberrisico's en deelt inzichten in een pragmatische aanpak om deze groeiende uitdagingen effectief te beheren.

Met jarenlange ervaring in wereldwijde organisaties zal Raffaele niet alleen de huidige stand van zaken bespreken, maar ook praktische handvatten bieden voor het bouwen van een veerkrachtige cyberbeveiligingsstrategie. Een inspirerende sessie voor iedereen die verder wil kijken dan de dagelijkse dreigingen en wil bouwen aan een veilige digitale toekomst.

kpn

PROGRAMMA
NLSECURE[ID]
2025

VOLGENDE TALK »

GREEN TALKS

PAULINE MALEK

SENIOR LEGAL ADVISOR
NCSC-NL

MIETTA GROENEVELD

DIRECTOR NATO C2COE
MINISTERIE VAN DEFENSIE

Internationale cyberdreigingen, afschrikking, en samenwerking
Geopolitieke conflicten raken heel Europa, ook Nederland. De oorlog die Rusland voert tegen Oekraïne beïnvloedt onze economische en digitale veiligheid, terwijl statelijke actoren ons voortdurend aanvallen in het cyberdomein. Met de toenemende dreiging is het cruciaal om Europa autonomer te maken, en onze kritieke infrastructuur te beschermen. In deze talk onderzoeken Pauline Malek (NCSC) en Kolonel Mietta Groeneveld (NATO C2COE) hoe hybride oorlogvoering moderne conflicten herdefinieert, en hoe de NAVO afschrikwekkend optreedt tegen dergelijke dreigingen die plaatsvinden in de 'grey zone'. Een sterke publiek-private samenwerking is essentieel om onze weerbaarheid te vergroten en cyberveiligheid te waarborgen.

PROGRAMMA
NLSECURE[ID]
2025

VOLGENDE TALK »

GREEN TALKS

JERRY LOMAN

PROGRAM MANAGER
NEDERLANDSE SPOORWEGEN

ÜMIT YILMAZ

MANAGING CONSULTANT
NEDERLANDSE SPOORWEGEN
(TRIPLE-ID)

De IAM-reis van de NS

De Nederlandse Spoorwegen werken hard aan de implementatie van hun cybersecurity-roadmap. In een continu veranderende digitale omgeving is het essentieel om flexibel in te spelen op nieuwe inzichten en dreigingen. Dit heeft grote invloed op het Identity & Access Management (IAM) binnen NS, een cruciaal onderdeel van digitale veiligheid. In deze sessie nemen Jerry Loman en Ümit Yilmaz je mee in de ontwikkelingen, uitdagingen en lessen van de IAM-reis van NS in de afgelopen jaren.

PROGRAMMA
NLSECURE[ID]
2025

VOLGENDE TALK »

GREEN TALKS

HENK BIJSTERBOSCH

TEAM MANAGER KENNISPARTNERS & MARKTPARTIJEN
SAMEN DIGITAAL VEILIG

NIS2 verplicht beveiliging en samenwerking met je leveranciers
De NIS2-richtlijn, die binnenkort zal worden omgezet in de Cyberbeveiligingswet, stelt dat essentiële en belangrijke entiteiten de beveiliging van hun toeleveringsketen zorgvuldig moeten regelen. Tijdens deze talk deelt Henk alles wat je moet weten over de cruciale rol van ketenverantwoordelijkheid in cybersecurity. Je krijgt inzicht in de tools en maatregelen die je moet implementeren, waarom deze van vitaal belang zijn voor de bescherming van je organisatie, en hoe je deze ketenverantwoordelijkheid op een structurele manier kunt aanpakken. Een sessie die je niet alleen informeert, maar ook praktische handvatten biedt om je beveiliging met leveranciers te versterken en zo de risico's in je toeleveringsketen te verkleinen.

kpn

VOLGENDE TALK »

BLACK TALKS

MARK EVENBLIJ

CO-FOUNDER & COO
DUCKDUCKGOOSE

Deepfakes: de grootste dreiging van AI-gedreven criminaliteit
Mark neemt je mee in de wereld van deepfakes, een van de meest ernstige en snelgroeiende bedreigingen op het snijvlak van kunstmatige intelligentie en cybercriminaliteit. Van financiële fraude tot grootschalige desinformatiecampagnes, deepfakes worden op steeds slimmere manieren ingezet om identiteiten te manipuleren, instellingen te misleiden en vertrouwen te ondermijnen.

Aan de hand van praktijkvoorbeelden laat Mark zien hoe synthetische media worden ingezet als krachtig wapen en bespreekt hij de nieuwste detectiemethoden en samenwerkingsstrategieën. Deze presentatie biedt concrete inzichten en handvatten om de risico's van deepfakes effectief te beperken en organisaties weerbaarder te maken tegen deze moderne vorm van digitale misleiding.

kpn

PROGRAMMA
NLSECURE[ID]
2025

VOLGENDE TALK »

BLACK TALKS

REINDER WOLTHUIS

SENIOR PROJECTMANAGER & CONSULTANT
TNO

SOC of the future: hoe ziet een Security Operations Center eruit in 2030?
Deze presentatie biedt een exclusieve blik op de toekomst van Security Operations Centers (SOC). TNO heeft zowel de huidige als de verwachte trends in cybersecurity geanalyseerd en deze vertaald naar een gedetailleerde SOC 2030-blauwdruk.
Deze blauwdruk schetst hoe SOC's er in 2030 uit zullen zien en welke technologische, organisatorische en maatschappelijke ontwikkelingen een rol zullen spelen.
Reinder zal tijdens deze sessie de onderzoeksresultaten presenteren en de meest opvallende elementen van de blauwdruk belichten, zoals de impact van kunstmatige intelligentie, de rol van samenwerking binnen de keten, en de verschuivingen in de beveiligingsstrategieën van organisaties. Een must-see voor iedereen die geïnteresseerd is in de toekomst van cybersecurity en wil begrijpen hoe SOC's zich de komende jaren zullen ontwikkelen.

kpn

PROGRAMMA
NLSECURE[ID]
2025

VOLGENDE TALK »

BLACK TALKS

OLAF HARTONG

SECURITY RESEARCHER
FALCONFORCE

Detection Engineering: lessen uit mislukkingen die waardevol bleken
Detection Engineering is een tijdrovend en technisch complex vakgebied dat diepgaand onderzoek, geduld en een flinke dosis doorzettingsvermogen vereist. In deze presentatie deelt Olaf zijn aanpak voor het onderzoeken en ontwikkelen van effectieve detectiestrategieën. Dit proces verloopt echter niet altijd soepel; bij het analyseren van moeilijk te detecteren technieken belanden we vaak in rabbit holes die uiteindelijk op niets uitlopen. Toch zijn deze mislukkingen niet zonder waarde. Falen blijkt vaak een uitstekende leermeester te zijn en biedt inzichten die anders verborgen zouden blijven. Deze sessie biedt een eerlijke en open blik op de uitdagingen van Detection Engineering en laat zien hoe mislukkingen niet alleen leerzaam, maar ook een essentieel onderdeel zijn van succes in dit vakgebied.

kpn

PROGRAMMA
NLSECURE[ID]
2025

VOLGENDE TALK »

BLACK TALKS

NICOLE VAN DER MEULEN

CYBERSECURITY INNOVATION LEAD
SURF

Quantum komt: de toekomst is nu

De quantumrevolutie lijkt misschien nog ver weg, maar de impact ervan begint nu al voelbaar te worden. Quantumtechnologie belooft enorme vooruitgang in rekenkracht, maar brengt tegelijkertijd grote risico's met zich mee voor onze digitale veiligheid. Quantumcomputers zullen in staat zijn om huidige encryptietechnieken, zoals RSA, te kraken, wat gevoelige gegevens en kritieke systemen wereldwijd kwetsbaar maakt. Hoewel de technologie zich nog in de ontwikkelingsfase bevindt, is het nu al essentieel om actie te ondernemen. Wacht je tot 2030, dan ben je te laat. In deze talk legt Nicole uit waarom de dreiging urgent is en waarom de transitie naar quantumveilige cryptografie nú moet beginnen. Ontdek wat jij kunt doen om voorbereid te zijn op de toekomst van cybersecurity.

kpn

PROGRAMMA
NLSECURE[ID]
2025

VOLGENDE TALK »

BLUE TALKS

CHRISTINA HOEFER

VP OF STRATEGY
FORESCOUT TECHNOLOGIES

De toekomst van OT-beveiliging
In deze sessie duikt Christina dieper in de risico's van Operational Technology (OT) en het Internet of Things (IoT). Ze bespreekt de laatste inzichten in dreigingsinformatie en onderzoek, en verkent manieren om proactief risico's te beheren. Daarnaast wordt gekeken naar de samenwerking tussen IT en OT om duurzame strategieën te ontwikkelen voor een algehele cyberweerbaarheid. Een belangrijke sessie voor iedereen die wil begrijpen hoe de integratie van OT en IT nieuwe uitdagingen creëert en hoe organisaties zich kunnen voorbereiden op de toekomstige beveiligingsbehoeften.

kpn

VOLGENDE TALK »

BLUE TALKS

ROBERT TOM

CYBERSECURITY EVANGELIST
FORTINET

Threat Intelligence: van inzicht naar actie
In een wereld vol geavanceerde cyberdreigingen is Threat Intelligence essentieel om aanvallers een stap voor te blijven. Tom legt uit hoe wereldwijd dreigingsinformatie wordt verzameld, geanalyseerd en vertaald naar bruikbare inzichten voor beveiligingsoplossingen. Aan de hand van het MITRE ATT&CK Framework laat Tom zien hoe elke fase van een aanval wordt aangepakt— van initiële toegang tot command-and-control communicatie en data-exfiltratie.

Daarnaast bespreekt hij hoe dreigingsinformatie niet alleen helpt bij het detecteren van lopende aanvallen, maar ook bij het voorspellen en voorkomen van toekomstige dreigingen. Deze sessie biedt praktische inzichten in hoe organisaties met Threat Intelligence proactief risico's kunnen beperken en hun beveiliging kunnen versterken.

kpn

VOLGENDE TALK »

BLUE TALKS

ROBBERT KELDER

CHIEF TECHNOLOGY OFFICER
INSPARK

Cybersecurity trends en strategieën:
een Deepdive in het Digital Defense Report van Microsoft

In deze presentatie onderzoekt Robbert de laatste bevindingen uit de uitgebreide analyse van het huidige cyberdreigingslandschap door Microsoft. Deelnemers krijgen inzicht in opkomende trends in cyberdreigingen, effectieve verdedigingsstrategieën en best practices voor het versterken van de veerkracht van organisaties. Door middel van praktijkgerichte casestudy's en data gestuurde inzichten, heeft deze sessie als doel cybersecurityprofessionals en andere belanghebbenden te voorzien van de kennis die nodig is om de complexiteit van moderne cyberdreigingen te begrijpen en te beheersen.

kpn

PROGRAMMA
NLSECURE[ID]
2025

BLUE TALKS

ANDY QUAEYHAEGENS

SOLUTION ENGINEER
NETSKOPE

Secure Connect als de enabler van secure success
Secure Connect, een oplossing gebaseerd op Zero Trust-technologie, ondersteunt organisaties bij het versterken van hun beveiliging en het verbeteren van operationele processen. Andy illustreert dit met praktische voorbeelden die laten zien hoe bedrijven beter beschermd kunnen worden tegen cyberdreigingen en tegelijkertijd efficiënter kunnen werken.

De oplossing maakt het mogelijk om Generative AI veilig toe te passen, risico's binnen de organisatie in kaart te brengen en bewustzijn te creëren over de mogelijke gevaren van digitale interacties. Secure Connect helpt bij het inschatten van risico's per transactie. Dit stelt organisaties in staat weloverwogen beslissingen te nemen over beveiliging, de continuïteit van bedrijfsprocessen te waarborgen en risico's te beheren.

kpn

PROGRAMMA NLSECURE[ID] 2025

LIVE OP LOCATIE

ANGRY NERDS PODCAST

De Angry Nerds-podcast, een levendige en vaak humoristische tech-podcast waarin een groep enthousiaste nerds actuele technologie-, IT- en cybersecurity-onderwerpen bespreekt. De hosts combineren technische diepgang met luchtige gesprekken, scherpe humor en af en toe een flinke dosis cynisme. Verwacht gesprekken over alles van netwerkinfrastructuren tot softwareontwikkeling, van privacykwesties tot bizarre tech-trends. De podcast is toegankelijk voor zowel doorgewinterde tech-experts als nieuwsgierige luisteraars die willen begrijpen wat er speelt in de digitale wereld. Kortom: informatief, eigenzinnig en vooral heel vermakelijk!

kpn

PROGRAMMA NLSECURE[ID] 2025

THEMA'S NETWERKPLEIN

IDENTITY & ENDPOINTS

De toekomst van Identity & Endpoints draait om versterkte beveiliging via multi-factor authenticatie, biometrie en real-time monitoring. Endpointbeveiliging maakt gebruik van AI en gedragsanalyse om verdachte activiteiten snel te detecteren, waardoor ongeautoriseerde toegang en datalekken effectiever kunnen worden voorkomen. Identity management vormt de basis voor digitale transformatie en innovatie, doordat het zorgt voor veilige en efficiënte toegang tot systemen en data. Door identiteit centraal te stellen in de beveiliging, kunnen organisaties hun transformatie versnellen en de security verbeteren.

PROGRAMMA NLSECURE[ID] 2025

THEMA'S NETWERKPLEIN

DATA & DATA DELEN

Beter samenwerken, incidenten voorkomen of de bereikbaarheid van informatie verbeteren. Data delen kan veel deuren openen. Maar hoe doe je het veilig? En als je data met externen deelt, hoe houd je dan de controle? Nieuwe wet- en regelgeving stelt steeds vaker eisen op voor dataverwerking. NIS2, DORA of het IZA, veel organisaties hebben of krijgen ermee te maken. Dat betekent niet dat we maar minder data moeten delen; wel dat we goed moeten nadenken over hóé. En dat begint bij een veilige infrastructuur.

PROGRAMMA NLSECURE[ID] 2025

THEMA'S NETWERKPLEIN

VEILIGE CONNECTIVITEIT

Digitalisering begint met verbinding: van 5G en glas tot mobiel, WiFi en IoT. Hoe zorgen we dat deze connecties veilig blijven? Zeker in een wereld waar (OT-)systemen steeds meer verweven raken met IT-netwerken? We nemen je mee in het verhaal van veilige verbindingen. Want alleen met betrouwbare en weerbare netwerken kunnen we bouwen aan een toekomst waarin technologie ons écht vooruit helpt.

PROGRAMMA NLSECURE[ID] 2025

THEMA'S NETWERKPLEIN

ZERO TRUST

In de moderne digitale wereld speelt beveiliging een cruciale rol. Het Zero Trust-framework biedt een heldere benadering om veilige toegang tot systemen en data te waarborgen. Dit model gaat uit van het principe 'never trust, always verify' en helpt organisaties stapsgewijs toe te werken naar een solide beveiligingsarchitectuur. Door te focussen op continue verificatie en minimale toegangsrechten, draagt het Zero Trust-framework bij aan een robuuste en toekomstbestendige digitale omgeving.

PROGRAMMA
NLSECURE[ID]
2025

THEMA'S NETWERKPLEIN

CLOUD & SECURITY

In de hybride werkomgeving van vandaag zijn flexibiliteit en veiligheid essentieel. Een multicloudstrategie zorgt voor veilige en betrouwbare toegang tot tools en data, altijd en overal. Door de integratie van cloudplatformen worden niet alleen prestaties geoptimaliseerd en regelgeving nageleefd, maar blijft veiligheid op ieder niveau gewaarborgd.
Met persoonlijke ondersteuning en een sterke lokale aanwezigheid werk je aan een digitale werkplek die zowel veilig, flexibel als toekomstbestendig is.

PROGRAMMA NLSECURE[ID] 2025

THEMA'S NETWERKPLEIN

FUTURE MONITORING

De toekomst van monitoring in cybersecurity ligt in het gebruik van AI en machine learning om bedreigingen sneller te detecteren en automatisch te reageren. Traditionele, handmatige methoden maken plaats voor real-time, proactieve benaderingen die geïntegreerd zijn met andere beveiligingssystemen. Dit maakt een snellere identificatie en mitigatie van risico's mogelijk, met een grotere focus op privacy en bescherming van persoonsgegevens.

PROGRAMMA NLSECURE[ID] 2025

THEMA'S NETWERKPLEIN

CYBER VEERKRACHT

Waar internetcriminelen zich vroeger voornamelijk richtten op 'grote vissen', zijn het nu ook vaker kleinere ondernemingen die slachtoffer worden, meestal met grote gevolgen. Waar een groot bedrijf een verlies van tienduizenden euro's of enkele tonnen wel op kan vangen, kan het voor kleinere bedrijven het einde van hun ondernemersreis betekenen. Doodzonde. En onnodig, want als je basisveiligheid op orde is, kun je de meeste ellende al voorkomen.

PROGRAMMA NLSECURE[ID] 2025

THEMA'S NETWERKPLEIN

WERKEN BIJ KPN

Werken in de wereld van digitale beveiliging betekent bijdragen aan een veiligere toekomst. In een omgeving die continu in beweging is, krijg je de kans om de nieuwste technologieën te gebruiken en samen te werken met experts om de veiligheid van miljoenen mensen en bedrijven te waarborgen. Hier staat jouw expertise centraal, en krijg je de vrijheid om je vaardigheden verder te ontwikkelen en nieuwe uitdagingen aan te gaan. Als je gepassioneerd bent over cybersecurity en wilt werken aan innovatieve oplossingen die de digitale wereld beschermen, is dit de plek voor jou om impact te maken en je carrière naar een hoger niveau te tillen.

PROGRAMMA
NLSECURE[ID]
2025

AANWEZIGE PARTNERS

CHECK POINT
cisco Partner
corelight
FORESCOUT See it. Secure it. Assure it.
IDlayr
infoblox
INSPARK
CEQUENCE
paloalto NETWORKS
SAMSUNG
THALES Building a future we can all trust
TREND MICRO
elastic
FORTINET
ONE IDENTITY by Quest
Microsoft
netskope
RANGE FORCE
trustwise AI Trust Simplified.
ubiqu

kpn

PROGRAMMA
NLSECURE[ID]
2025

ONLINE PLATFORM

ON-DEMAND

Een week na het event zijn zowel de keynotes als alle talks beschikbaar op het online platform van NLSecure[ID]. Via dit platform kun je niet alleen de sessies terugkijken, maar ook in contact komen met KPN's securityexperts en onze partners.

Kun jij er dus op 21 januari niet bij zijn of wil je alles nog eens rustig terugkijken? Meld je dan alsnog aan om het event vanaf 28 januari online te bekijken.