NEXUS 7
RISK ASSESSMENT

Van Kwetsbaarheid naar Kracht

Transformeer Cybersecurity-gedrag met NEXUS-7

Een evidence-based benadering van de menselijke factor in cybersecurity

Executive Summary

In een tijd waarin technologie steeds beter beveiligd is, blijft **menselijk gedrag de bepalende factor** voor cybersecurity. Een enkele klik op een phishingmail, het negeren van regels of onzorgvuldig omgaan met vertrouwelijke informatie kan ernstige risico's veroorzaken – ondanks miljoeneninvesteringen in technische beveiliging.

NEXUS-7 helpt organisaties om cybersecurity van een kwetsbaarheid naar een kracht te transformeren, door gedrag van medewerkers inzichtelijk te maken en proactief te beïnvloeden. Onze gevalideerde,

Direct meetbare resultaten

✅ **Minder cyberincidenten** door bewust, veilig gedrag
✅ **Zelfsturende medewerkers** die veilig handelen
✅ **Continu verbeterproces** met meetbare voortgang
✅ **Data-gedreven beleid** voor gerichte maatregelen

Wat NEXUS-7 uw organisatie biedt

Evidence-based gedragsanalyse die risico's meetbaar en zichtbaar maakt:
- Herken vroegtijdig rode vlaggen in gedrag
- Gestructureerde ontwikkelcyclus voor duurzame gedragsverandering
- Individueel én organisatorisch inzicht voor gerichte acties
- Continue verbetercyclus, geen eenmalige training

Het Punt van Verbetering: De Menselijke Factor

Waarom technologie alleen niet genoeg is

Cybersecurityproblemen bedreigen niet alleen data en systemen, maar ook **financiële stabiliteit, bedrijfscontinuïteit, vertrouwen en strategische posities** van organisaties. Terwijl organisaties jaarlijks miljarden investeren in technische beveiligingsmaatregelen, blijft menselijk gedrag de zwakste schakel.

De harde feiten:

- 95% van alle cyberincidenten wordt veroorzaakt door menselijke fouten
- Een gemiddeld datalek kost Nederlandse organisaties €3,9 miljoen
- 60% van de getroffen bedrijven verliest klanten na een incident

De uitdaging: Diepgewortelde gedragspatronen

Medewerkers vertonen vaak **diepgewortelde gedragspatronen** die zowel kansen als risico's met zich meebrengen:

Gedragspatroon	Positief Effect	Cybersecurity Risico
Impulsiviteit	Snel schakelen, probleemoplossend	Klikken zonder nadenken, phishing
Perfectionisme	Nauwkeurig, gedetailleerd	Vermijding van nieuwe systemen
Regelafwijzing	Creatief, innovatief	Omzeilen van beveiligingsprotocollen
Stressgevoeligheid	Empathisch, betrokken	Fouten onder druk, sociale manipulatie
Conflictvermijding	Harmonie, teamspeler	Niet rapporteren van incidenten

NEXUS 7
RISK ASSESSMENT

Deze patronen kunnen positieve effecten hebben, zoals veerkracht en stressbestendigheid, maar ook negatieve gevolgen voor cyberveilig gedrag.

Het her(er)kennen van 'rode vlaggen' in cybersecurity-gedrag is een cruciale eerste stap richting verandering.

Wat huidige oplossingen missen

Traditionele cybersecurity-trainingen falen omdat ze:

- ❌ Eenmalig zijn, zonder follow-up of herhaling
- ❌ Generiek zijn, niet afgestemd op individueel gedrag
- ❌ Kennis overdragen, maar geen gedragsverandering bewerkstelligen
- ❌ Niet meten wat het effect is op werkelijk gedrag
- ❌ Geen inzicht geven in onderliggende drivers

De Oplossing: NEXUS-7 Security Gedragsanalyse

NEXUS-7 biedt een **gestructureerde, wetenschappelijk onderbouwde oplossing** om cyber(on)veilig gedrag te detecteren, analyseren en duurzaam te veranderen. Onze Security Gedragsanalyse biedt zichtbaarheid, inzicht, detectie, waarschuwing en bescherming tegen cyberdreigingen door afwijkend gedrag te monitoren en input voor gedragsverandering te leveren.

Drie pijlers van de NEXUS-7 aanpak

1. **Inzicht in Gedrag**

   Wetenschappelijk onderbouwd inzicht in hoe medewerkers omgaan met cybersecurity. In slechts 18 minuten krijgt u:

   - Individueel gedragsprofiel over 7 kritieke niveaus
   - Analyse van 11 specifieke impact-gebieden
   - Identificatie van persoonlijke rode vlaggen
   - Vergelijking met organisatie-benchmark

2. **Input voor Actie**

   Concrete handvatten om gericht gedrag te beïnvloeden:

   - Gepersonaliseerde aanbevelingen per medewerker
   - Management dashboards voor teams en afdelingen
   - Prioritering van interventies op basis van risico
   - Praktische tips en actiepunten voor direct gebruik

1. **GROW! - Duurzame Gedragsverandering**

   Structurele ontwikkeling richting blijvend veilig handelen:

   - Continue feedbackloop via herhaalde metingen
   - Zelfsturende medewerkers die eigen gedrag monitoren
   - Trainingen en coaching afgestemd op persoonlijk profiel
   - Meetbare voortgang over tijd

Het NEXUS-7 platform: Intelligence meets usability

Onze Cybersecurity gedragsaanpak combineert een geavanceerde SaaS-oplossing (Software als dienst), ontwikkelt door Roger Heykoop, met wetenschappelijke diepgang, gecreëerd door Nina Binnendijk, met gebruiksgemak:

Voor Medewerkers

- **Q-sort assessment** in 18 minuten via intuïtieve drag-and-drop interface
- Persoonlijk rapport met positief geformuleerde inzichten
- Tweetalige ondersteuning (Nederlands/Engels)
- Mobiel-vriendelijk, toegankelijk vanaf elk apparaat

Voor HR & Management

- **Real-time dashboards** met organisatie-overzicht
- Exporteerbare rapporten (PDF, Excel, CSV)
- Benchmark-vergelijkingen tussen teams en afdelingen
- Trend-analyse voor lange termijn monitoring
- AI-gegenereerde aanbevelingen per cluster

Voor IT & Security Officers

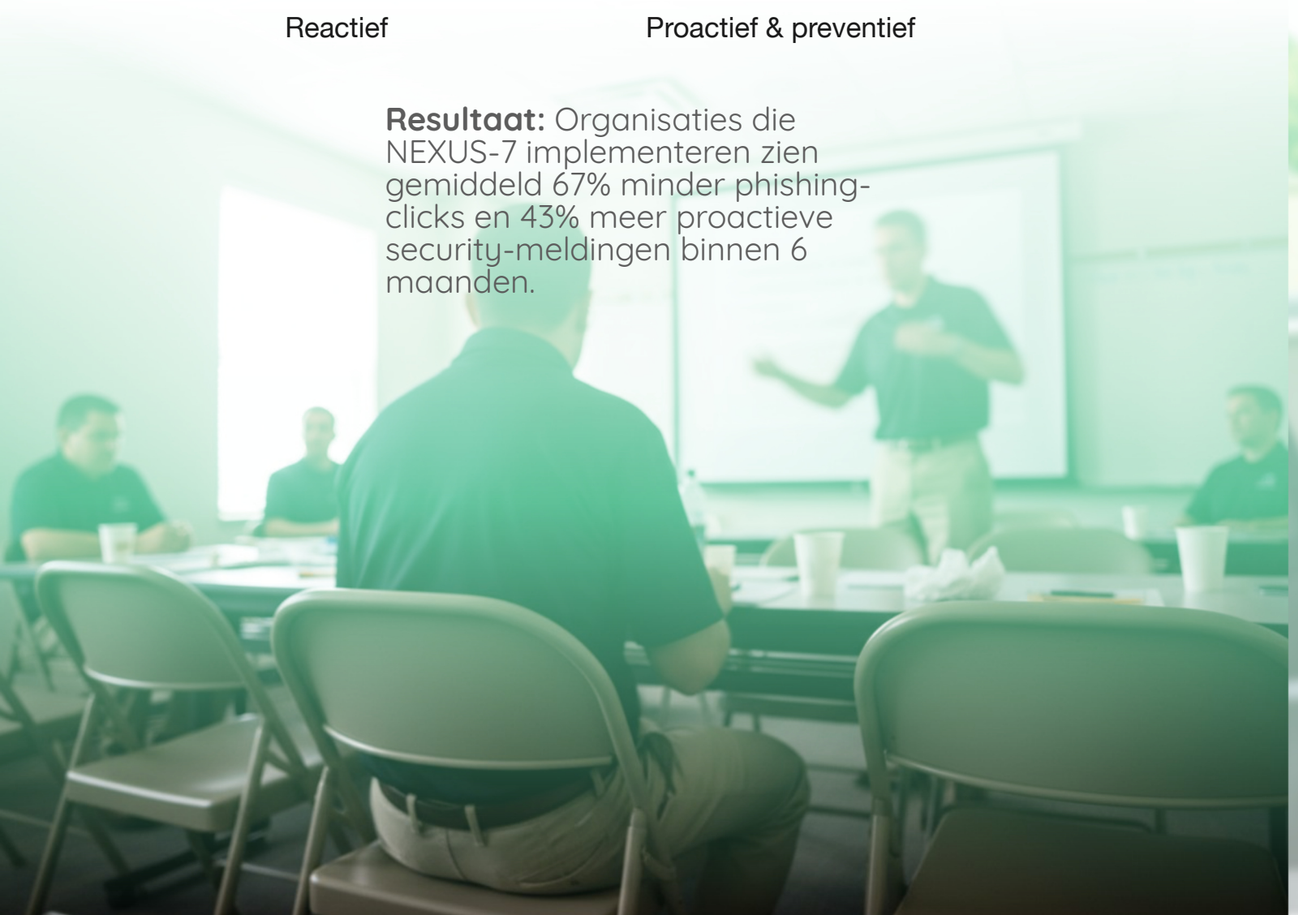
- Identificatie van hoogrisico-groepen
- Gedetailleerde impact-analyse (11 dimensies)
- Clustring van gedragspatronen voor efficiënte interventies
- API-integratie met bestaande security tools

De kracht van data-gedreven gedragsverandering

NEXUS-7 gaat verder dan traditionele awareness:

Traditionele Training	NEXUS-7 Gedragsanalyse
Eenmalig evenement	Continue cyclus
Generieke content	Gepersonaliseerde inzichten
Kennis-overdracht	Gedragsverandering
Geen meting	Objectieve data
Compliance-gericht	Ontwikkelings-gericht
Reactief	Proactief & preventief

Resultaat: Organisaties die NEXUS-7 implementeren zien gemiddeld 67% minder phishing-clicks en 43% meer proactieve security-meldingen binnen 6 maanden.



NEXUS7
RISK ASSESSMENT

Wetenschappelijke Basis: De Q-Methodologie

Gevalideerde onderzoekstechniek

De NEXUS-7 Security Gedragsanalyse is gebaseerd op de **gevalideerde Q-methodologie**, een wetenschappelijke onderzoekstechniek ontwikkeld door:

- **Prof. dr. W. Stephenson** (1902-1989): Grondlegger van Q-methodologie
- **Prof. dr. S. Brown** (1980: Political Subjectivity): Theoretische uitwerking
- **Prof. dr. M. Brouwer** (1929-2001): Nederlandse implementatie met drs. C.T.M. Binnendijk: Vanaf 2001: Universitair en commercieel (Q-Research, EnSemper). Founder Nexus-7.

Deze methodiek, met wortels in de psychologie en natuurkunde, heeft zich wereldwijd bewezen in uiteenlopende onderzoeksterreinen waaronder gedragspsychologie, organisatieontwikkeling en risicomanagement.

Waarom Q-methodologie uniek is

Wat de NEXUS-7 Security Gedragsanalyse uniek maakt, is dat kandidaten worden uitgedaagd om een rangordening van 42 cybersecuritystellingen te maken (prioriteiten aangeven) binnen een gestructureerd grid.

De kracht van geforceerde keuzes

Dit dwingt hen om **elke stelling te wegen ten opzichte van alle andere**, wat neerkomt op **minimaal 420 impliciete keuzes per kandidaat**. Door deze intensieve afweging ontstaat een gedetailleerd, genuanceerd inzicht (persoonlijk profiel) in individuele gedragsvoorkeuren in cybersecuritycontexten.

Waarom dit werkt:

- Mensen kunnen niet alle stellingen als “belangrijk” markeren
- Gedwongen prioritering onthult werkelijke waarden
- Impliciete keuzes zijn moeilijker te manipuleren
- Resultaat is veel rijker dan likert-schaal vragenlijsten

Van data naar inzicht

De 42 stellingen zijn zorgvuldig verdeeld over:

- **7 niveaus** (drivers) van de NEXUS-7 Ontwikkelcyclus (6 stellingen per niveau)
- **11 impacts** die cybersecurity-gedrag beïnvloeden (3-4 stellingen per impact)
- **Perfecte balans** tussen positief en negatief geformuleerde stellingen (21/21)

Deze wetenschappelijke verdeling zorgt voor **valide, betrouwbare metingen** die herhaalbaar en vergelijkbaar zijn.

De NEXUS-7 Ontwikkelcyclus

Zeven Drivers voor Gedragsverandering

De cybersecuritystellingen in de Security Gedragsanalyse zijn zorgvuldig verdeeld over de **zeven drivers (niveaus) van de NEXUS-7 Ontwikkelcyclus**.

Dit model, gebaseerd op het **Linguïstisch Programmeermodel** (prof. dr. G. Bateson, 1904-1980; R. Dilts, NLP), beschrijft zeven hiërarchische niveaus die invloed hebben op gedragsverandering.

Het fungeert als een analyse-, verander-, zelfregulatie-, training- en coachingmodel, dat kandidaten helpt inzicht te krijgen in hun persoonlijke drivers richting missiegericht, veilig securitygedrag.

1. Omgeving (Context)

De fysieke en digitale context waarin medewerkers opereren.

- **Voorbeelden:** Werkplek, systemen, tools, procedures
- **Interventies:** Technische voorzieningen, proces-optimalisatie

2. Gedrag (Acties)

De zichtbare acties en keuzes die medewerkers maken.

- **Voorbeelden:** Wachtwoord-gedrag, e-mail controle, meldingen doen
- **Interventies:** Gedragstraining, simulaties, feedback

3. Capaciteiten (Vaardigheden)

De vaardigheden en competenties die nodig zijn voor veilig gedrag.

- **Voorbeelden:** Phishing herkennen, beveiligingssoftware gebruiken, risico inschatten
- **Interventies:** Skill-training, oefeningen, certificeringen

De Hiërarchische Structuur

Elke volgende driver in de cyclus bouwt voort op de vorige, waardoor gedrag systematisch kan worden ontwikkeld en versterkt:

7. MISSIE & VISIE
↓
6. EIGEN IDENTITEIT
↓
5. SOCIALE IDENTITEIT
↓
4. OVERTUIGINGEN & WAARDEN
↓
3. CAPACITEITEN
↓
2. GEDRAG
↓
1. OMGEVING

4. Overtuigingen & Waarden (Mindset)

De diepere overtuigingen die gedrag sturen.

- **Voorbeelden:** “Security is belangrijk”, “Ik ben verantwoordelijk”, “Melden is normaal”
- **Interventies:** Mindset-coaching, cultuurverandering, storytelling

5. Sociale Identiteit (Zelfbeeld vanuit de groep)

Hoe medewerkers Cybersecurity zien vanuit de groep (teams, afdelingen).

- **Voorbeelden:** “Als de rest van het team zegt dat deze procedure veilig is, volg ik dat gewoon”, “Ik stel geen vragen over de nieuwe securityregels, iedereen volgt ze toch al”
- **Interventies:** Workshops over feedback geven en vragen stellen, Rollenspellen waarbij men “nee” zegt of afwijkende ideëen aandraagt. Coaching.

6. Eigen Identiteit (Zelfbeeld)

Hoe medewerkers zichzelf zien in relatie tot cybersecurity.

- **Voorbeelden:** “Ik ben een security-bewuste professional”, “Ik ben een rolmodel”
- **Interventies:** Identiteits-coaching, ambassadeursprogramma's

7. Missie & Visie (Purpose)

Het hogere doel waarvoor cybersecurity dient.

- **Voorbeelden:** Beschermen van klanten, bijdragen aan maatschappij, organisatiedoelen
- **Interventies:** Purpose-alignment, leiderschap, strategie

Continue Verbetering

De Ontwikkelcyclus maakt zichtbaar hoe **concrete stappen leiden tot gedragsverandering**. Iedere volgende driver in de cyclus helpt kandidaten een stap verder in hun ontwikkeling naar cyberveilig gedrag, waardoor het proces van gedragsaanpassing systematisch en meetbaar wordt ondersteund.

Door het proces **regelmatig te doorlopen, te meten en monitoren**, ontstaat een **continu verbeterproces**. Zo wordt cyberveilig gedrag duurzaam geïntegreerd in de dagelijkse praktijk.

Impacts op Cybersecurity-gedrag

Elf Specifieke Beïnvloedingsfactoren

Bij NEXUS-7 noemen we de individuele factoren die gedrag binnen de drivers beïnvloeden **impacts**. Impacts stimuleren veilig of onveilig gedrag en werken op twee niveaus:

1. Bewuste Keuzes

- **Attitude:** Houding ten opzichte van cybersecurity
- **Zelfeffectiviteit:** Vertrouwen in eigen veiligheidsgedrag
- **Risicoperceptie:** Inschatten van dreigingen

2. Automatische Reacties

- **Gewoontes:** Geautomatiseerd gedrag
- **Stressreacties:** Gedrag onder druk
- **Sociale beïnvloeding:** Impact van collega's en cultuur

De 11 Impact-gebieden

Elke medewerker krijgt een score op deze 11 impact-gebieden, die specifieke aanknopingspunten bieden voor gerichte interventies:

1	**E-mail Security:**	Omgang met verdachte berichten
2	**Wachtwoord Management:**	Gebruik en bescherming van credentials
3	**Social Engineering:**	Weerbaarheid tegen manipulatie
4	**Data Bescherming:**	Omgang met vertrouwelijke informatie
5	**Device Security:**	Beveiliging van apparaten
6	**Netwerk Beveiliging:**	Veilig gebruik van netwerken
7	**Software Updates:**	Tijdig updaten van systemen
8	**Physical Security:**	Fysieke beveiligingsmaatregelen
9	**Incident Rapportage:**	Melden van verdachte zaken
10	**Compliance Naleving:**	Volgen van regels en procedures
11	**Security Awareness:**	Algemeen beveiligingsbewustzijn

Verankering: Van Inzicht naar Gewoonte

Impacts bieden **concrete aanknopingspunten voor interventies** die medewerkers helpen om veilig gedrag structureel te verankeren.

Verankering – het duurzaam maken van een nieuw gedrag of patroon – is essentieel voor cyberveilig gedrag, zodat het onderdeel wordt van iemands dagelijkse routines en automatisch wordt toegepast. Een combinatie van zowel **zelfreflectie als externe ondersteuning** (coaching of trainingen), waarborgt duurzame verandering.

NEXUS7
RISK ASSESSMENT

De NEXUS-7 Voordelen

Waarom Organisaties voor NEXUS-7 Kiezen

De NEXUS-7 aanpak biedt aantoonbare voordelen ten opzichte van bestaande oplossingen:

✅ **Dieper Inzicht in Menselijk Gedrag**

In slechts **18 minuten** een compleet persoonlijkheidsprofiel op 7 niveaus en 11 impacts – veel rijker dan traditionele vragenlijsten.

✅ **Voorspellende Kracht**

Identificeer **rode vlaggen** voordat ze leiden tot incidenten. Proactief ingrijpen in plaats van achteraf reageren.

✅ **Personalisatie op Schaal**

Unieke inzichten per medewerker, gecombineerd met **efficiënte clustering** voor organisatie-brede interventies.

✅ **Sneller Signaleren van Problemen**

Real-time dashboards tonen direct **hoogrisico-groepen en trends**, zodat u snel kunt handelen.

✅ **Verbeterde Effectiviteit van Interventies**

Gerichte trainingen op basis van **data-gedreven inzichten** verhogen effectiviteit met 3-5x ten opzichte van generieke awareness.

✅ **Objectief en Data-gedreven**

Wetenschappelijk onderbouwde metingen elimineren **subjectiviteit en bias** uit beoordelingen.

✅ **Continue Optimalisatie**

Herhaalde metingen tonen **meetbare voortgang** en stellen bij waar nodig – een echte verbetercyclus.

Return on Investment

Directe kostenbesparingen:

- Voorkoming van één gemiddeld datalek: €3,9 miljoen
- Reductie helpdesk-calls door veiliger gedrag: 15-30%
- Verminderde uitval door malware-infecties: 40-60%
- Lagere compliance-boetes door naleving: tot 4% omzet

Indirecte waardecreatie:

- Versterkt klantvertrouwen en reputatie
- Concurrentievoordeel in security-gevoelige sectoren
- Verbeterde employee engagement en veiligheidscultuur
- Aantoonbare compliance voor saudits en certificeringen

Snelle implementatie: - Operationeel binnen 2-4 weken - Eerste resultaten zichtbaar binnen 1 maand - ROI positief binnen 3-6 maanden

Implementatie & Gebruik

Vier Stappen naar Succesvol Gedragsverandering

Stap 1:
Baseline Meting (Week 1-2)

- Uitrol assessment naar alle medewerkers
- Individuele profielen en organisatie-overzicht
- Identificatie van rode vlaggen en risico-groepen

Stap 2:
Analyse & Planning (Week 3-4)

- Management workshops voor bespreking resultaten
- Prioritering van interventies op basis van risico
- Ontwikkeling van gepersonaliseerde actieprogramma's

Stap 3:
Interventie & Training (Maand 2-6)

- Uitvoering gerichte trainingen per cluster
- Individuele coaching voor hoogrisico-medewerkers
- Implementatie van proces- en technische verbeteringen

Stap 4:
Monitoring & Optimalisatie (Continu)

- Kwartaal herhalings-metingen voor voortgang
- Bijstelling interventies op basis van data
- Continue verbetering van security-cultuur

Flexibele Pricing voor Elke Organisatie

NEXUS-7 biedt **schaalbare, transparante prijsmodellen** die meegroeien met uw behoeften:

Eenmalige Assessments

Perfecte voor pilotprojecten of eenmalige metingen:

- Volume discount: hoe meer tests, hoe lager de prijs per test
- Vanaf €25/test (kleine volumes) tot €7,50/test (grote volumes)
- 10 pricing tiers voor optimale flexibiliteit

Subscription Modellen

Voor organisaties die continue monitoring willen:

- Maandelijks, halfjaarlijks of jaarlijks abonnement
- Onbeperkt aantal assessments binnen periode
- Inclusief API-toegang en premium support

Enterprise Oplossingen

Voor grote organisaties met specifieke eisen:

- Custom implementation en integratie
- Dedicated success manager
- White-label mogelijkheden
- On-premise deployment optie

Voor Wie is NEXUS-7?

Ideale Doelgroepen

NEXUS-7 is ontwikkeld voor organisaties die cybersecurity serieus nemen en de menselijke factor willen versterken:

Grote Enterprises (1000+ medewerkers)

- Complex beveiligingslandschap met diverse afdelingen
- Noodzaak tot continue compliance en audits
- Budget voor structurele security-investeringen

Middelgrote Organisaties (100-1000 medewerkers)

- Groeiende security-behoeften zonder dedicated CISO
- Efficiënte aanpak nodig met meetbare resultaten
- Focus op kosteneffectiviteit en ROI

Security-gevoelige Sectoren

- **Financiële dienstverlening:** banken, verzekeraars, fintech
- **Gezondheidszorg:** ziekenhuizen, zorgverzekeraars, medtech
- **Overheid:** ministeries, gemeenten, uitvoeringsorganisaties
- **Technologie:** software-bedrijven, managed service providers
- **Industrie:** productie met kritieke infrastructuur

Partners & Resellers

- **Security consultants** die toegevoegde waarde zoeken
- **IT-dienstverleners** met security-propositie
- **Training & development** organisaties
- **HR-adviseurs** met focus op organisatieontwikkeling

Technologie & Platform

Modern SaaS Platform

NEXUS-7 is gebouwd door Roger Heykoop, Founder Nexus-7, oprichter van diversie internetproviders en voormalig lead developer en lead architect van DigiD. als een state-of-the-art. Nexus-7 is een **Software-as-a-Service platform** met enterprise-grade beveiliging en schaalbaarheid:

Technische Specificaties

- **Multi-tenant architectuur** voor schaalbaarheid
- **99.9% uptime** SLA met redundante infrastructuur
- **GDPR-compliant** data processing en opslag

Integratie Mogelijkheden

- **RESTful API** voor custom integraties
- **SSO ondersteuning** (SAML, OAuth) voor seamless login
- **Export functionaliteit** (PDF, Excel, CSV) voor rapportages
- **Webhook notificaties** voor real-time updates
- **Embedding opties** voor white-label implementaties

User Experience

- **Responsive design** voor desktop, tablet en mobiel
- **Intuïtieve drag-and-drop** interface voor Q-sort
- **Tweetalige ondersteuning** (Nederlands/Engels)
- **Accessibility compliant** (WCAG 2.1 AA)
- **Dark mode** voor comfortabel gebruik

Security & Privacy

- **ISO 27001** certified infrastructuur
- **End-to-end encryptie** voor gevoelige data
- **Role-based access control** (RBAC) voor data-governance
- **Audit logging** voor compliance tracking
- **Data residency** binnen EU

Privacy en AVG/GDPR Compliance: Veiligheid zonder Compromissen

Privacy by Design – niet als bijgedachte, maar als fundament.

Bij Nexus-7 begint veiligheid bij het ontwerp: ons systeem werkt zonder persoonsgegevens. Punt. U bepaalt zelf hoeveel privacy u wilt borgen, van volledig anoniem tot identificeerbaar – altijd met volledige controle.

Drie flexibele privacy niveaus

Volledig Anonieme Assessments

Eén uitnodigingscode, gedeeld met uw team. Werknemers ontvangen een persoonlijk rapport, maar verder niemand – ook u niet – ziet individuele scores. Rapportages zijn uitsluitend op groepsniveau. Maximale privacy, bruikbare inzichten.

Herleidbare Assessments (met uw eigen sleutel)

Unieke codes per werknemer, maar de koppeling blijft in úw handen. Wij zien alleen codes, u beheert de identiteit. Volledige controle zonder dat gegevens onze systemen verlaten.

Niet-Anonieme Assessments (op verzoek)

Kiest u voor directe communicatie via e-mail? Dan gebruiken we persoonsgegevens uitsluitend voor testafname en verwijderen deze automatisch na rapportage. Een verwerkersovereenkomst (AVG-compliant) regelt alles waterdicht.

IJzeren Garanties

✅ **Geen verkoop, geen deling** – uw data blijft uw data

✅ **EU-only hosting** – gegevens verlaten nooit de Europese Unie

✅ **AI-proof** – geen enkele AI-dienst krijgt toegang tot klant- of werknemersgegevens

✅ **On-premise mogelijk** – wilt u Nexus-7 in uw eigen datacenter? Dat kan.

Privacy is geen feature. Het is een mentaliteit.

En bij Nexus-7 staat die mentaliteit centraal – zodat u kunt focussen op wat echt telt: **de ontwikkeling van uw team.**

Conclusie: Maak Cybersecurity een Kracht

Van Zwakste Schakel naar Sterkste Verdediging

Cybersecurity is veel meer dan alleen technologie – het is **in grote mate afhankelijk van menselijk gedrag**. Organisaties kunnen nog zo veel firewalls, antivirusprogramma's of geavanceerde systemen inzetten, maar de echte veiligheid wordt bepaald door hoe medewerkers dagelijks omgaan met informatie en digitale processen.

NEXUS-7 biedt een evidence-based, praktische en duurzame aanpak:

- Ondersteunt medewerkers actief bij het maken van veilige keuzes
- Detecteert afwijkend gedrag (rode vlaggen) voordat het escaleert
- Helpt risico's tijdig te identificeren en te mitigeren
- Transformeert security van compliance naar cultuur

Start Vandaag

Klaar om de Menselijke Factor te Versterken?

Transformeer uw cybersecurity van een kwetsbaarheid naar een kracht. Neem contact op voor een **vrijblijvende demo** of **pilot-implementatie** bij uw organisatie.

Contact:

Website: www.nexus-7.nl

E-mail: info@nexus-7.nl

De Drie Pijlers van Succes

Door **technologie, gedragswetenschap en continue verbetering** te combineren, stelt NEXUS-7 organisaties in staat om:

1. **Niet alleen te reageren, maar te voorkomen** – proactieve risicodetectie
2. **Niet alleen te trainen, maar te transformeren** – duurzame gedragsverandering
3. **Niet alleen te meten, maar te verbeteren** – data-gedreven optimalisatie

Maak Cybersecurity een Integraal Onderdeel

NEXUS-7 maakt cyberveiligheid een **integraal onderdeel van de organisatiecultuur en strategie**. Medewerkers werken ultiem aan cybersecurity wanneer ze **bewust, proactief en consistent** handelen volgens de beste veiligheidspraktijken, zodat risico's zo klein mogelijk blijven en de organisatie beschermd is.

De NEXUS-7 Gedragsanalyse realiseert dit voor uw organisatie.

Nexus-7
Lagedijk 11A
2064 KV Spaarndam
Nederland

+31 84 8332125
https://www.nexus-7.nl
info@nexus-7.nl