eutronix
innovate. automate. elevate.

www.eutronix.eu

WHITE PAPER

Cyberweerbaarheid versterken in Transport & Logistiek

—

NIS2-NALEVING MET SOTI ONE

SOTI ONE

WHITE PAPER

Cyberweerbaarheid versterken in Transport & Logistiek: NIS2-naleving met SOTI ONE

Executive Summary

De transport- en logistieke sector vormt het circulatiesysteem van onze economie – goederen en mensen worden verplaatst met een steeds grotere afhankelijkheid van digitale technologie. Van vrachtwagenchauffeurs die tablets gebruiken voor route-beheer tot magazijnen vol scanners en slimme sensoren: mobiliteit en IoT veranderen de werking van de sector fundamenteel. Maar deze digitale vooruitgang brengt ook nieuwe cyberrisico's met zich mee.

Omdat transport wordt erkend als kritieke infrastructuur, legt de NIS2-richtlijn van de EU strikte cybersecuritynormen op aan operators in de transport- en logistieke sector. Bedrijven moeten realtime gegevensuitwisseling beveiligen, hun toeleverings-ketens beschermen tegen inbreuken en voorbereid zijn op bedreigingen zoals ransomware die distributienetwerken kunnen stilleggen.

Dit white paper onderzoekt de specifieke uitdagingen waarmee logistieke bedrijven in West-Europa worden geconfronteerd onder NIS2 – waaronder het beheren van duizenden mobiele eindpunten in verschillende landen, het aanpakken van kwetsbaarheden via externe partners en het garanderen van 24/7 beschikbaarheid van leveringssystemen.

Vervolgens wordt uitgelegd hoe SOTI MobiControl en het SOTI ONE Platform deze uitdagingen rechtstreeks aanpakken. Belangrijke functies zoals gecentraliseerd apparaatbeheer, continue zichtbaarheid op apparaatstatus, remote troubleshooting en handhaving van beveiligingsbeleid worden belicht als sleutels tot zowel compliance als operationele efficiëntie.

We delen geanonimiseerde succesverhalen van logistieke bedrijven die met SOTI honderdduizenden euro's hebben bespaard – dankzij minder uitvaltijd, snellere implementaties en verbeterde beveiliging van hun mobiele vloot.

Voor CIO's, CISO's en operations managers in transport en logistiek biedt dit document een routekaart om van de NIS2-verplichting een kans te maken – om device management te moderniseren, de cybersecurityhouding te versterken en leveringen op schema te houden.

Een afsluitende sectie schetst concrete vervolgstappen zoals demo's, gidsen en compliance reviews om je traject naar NIS2-gereedheid te versnellen.

Introductie: Mobiliteit aan het stuur van de logistiek – en de risico's ervan

In de wereld van transport en logistiek zijn snelheid en efficiëntie cruciaal. Of het nu gaat om een transportbedrijf dat goederen over grenzen heen levert of een distributiecentrum dat de voorraad beheert – tijdige informatie-uitwisseling is essentieel. Vandaag verloopt die uitwisseling via mobiele computers, robuuste handhelds, voertuigtelematica en een waaier aan verbonden apparaten (barcodescanners, GPS-trackers, temperatuursensoren voor koeltransporten, enz.).

In zekere zin vormen deze eindpunten de nieuwe "bemanning" die ervoor zorgt dat pakketten op tijd aankomen en de operaties vlot verlopen.

Maar daartegenover staat dat de sector een aantrekkelijk doelwit is geworden voor cyberaanvallen. Een ransomware-aanval die het dispatchsysteem van een rederij platlegt of een datalek dat de gegevens van een spoorwegexploitant manipuleert, kan verregaande gevolgen hebben voor de samenleving – van vertraagde leveringen tot economische schade, en zelfs levensgevaar als essentiële goederen hun bestemming niet bereiken. Daarom erkent NIS2 transport als een essentiële sector en vereist het robuuste cybersecuritymaatregelen van alle operators.

Bedrijven moeten zowel hun IT- als OT-systemen (operationele technologie) beveiligen, de veiligheid van hun leveranciers beoordelen en de continuïteit van kritieke logistieke diensten waarborgen – zelfs in crisissituaties.

Voor IT-teams in de logistiek betekent dit het aanpakken van uitdagende vragen zoals:

- Hoe houden we duizenden mobiele toestellen, gebruikt door chauffeurs en magazijnmedewerkers, up-to-date en beveiligd zonder onze kleine IT-afdeling te overbelasten?
- Hoe kunnen we onmiddellijk ondersteuning bieden aan een chauffeur met een defecte navigatietablet op 500 km afstand?
- Zijn onze barcodescanners en voertuiggemonteerde apparaten beschermd tegen ongeautoriseerde toegang?
- En hoe bewijzen we aan regelgevers (en klanten) dat onze cyberbeveiliging en incidentrespons aan de nieuwe normen voldoen?

Deze inleiding schetst het speelveld voor transport- en logistieke bedrijven in België, Frankrijk, Nederland, Luxemburg en heel Europa. In de volgende secties gaan we dieper in op de NIS2-uitdagingen binnen deze sector, en hoe een oplossing voor centraal eindpuntbeheer de sleutel kan zijn tot zowel compliance als efficiëntere operaties.

Belangrijkste Cybersecurity- en Compliance-uitdagingen in Transport & Logistiek

1. **Geografisch verspreide mobiele vloot**
Logistieke bedrijven beschikken vaak over toestellen verspreid over meerdere landen – in vrachtwagens, havens, magazijnen en hubs. Het handmatig beheren en updaten van deze toestellen is vrijwel onmogelijk. Zorgen dat elk toestel voldoet aan de beveiligingsvoorschriften (juiste configuraties, recente patches) is een enorme uitdaging, zeker omdat chauffeurs voortdurend onderweg zijn en toestellen slechts sporadisch verbinding maken met het bedrijfsnetwerk.

2. **Ransomware en uitvalrisico's**
De transportsector wordt steeds vaker getroffen door ransomware, die routingsystemen, magazijnautomatisering of klantportalen kan verstoren. In tegenstelling tot sommige sectoren draait logistiek op strakke levertermijnen – enkele uren uitval kunnen al leiden tot achterstanden en contractbreuken. NIS2 verplicht bedrijven om het risico op dienstonderbreking tot een minimum te beperken. Dat vereist snelle noodherstelprocedures en de mogelijkheid om geïnfecteerde toestellen snel te isoleren en herstellen vóór de malware zich verspreidt.

3. **Kwetsbaarheden in de toeleveringsketen en bij derden**
Logistiek is per definitie collaboratief, met partners, onderaannemers en gekoppelde klantensystemen.
Een zwakke schakel in een apparaat van een derde partij (bijvoorbeeld een onveilige smartphone van een koerier) kan kwetsbaarheden introduceren in het hele netwerk. Nagaan of externe chauffeurs of 3PL-partners aan uw beveiligingsnormen voldoen, is moeilijk. NIS2 vereist het beoordelen en beheersen van deze externe risico's, wat betekent dat bedrijven beveiligingsmaatregelen moeten uitbreiden naar systemen die ze zelf niet volledig beheren.

4. **Toename van verbonden apparaten (IoT)**
Moderne logistieke operaties maken veel gebruik van IoT – telematicatoestellen in vrachtwagens, slimme vlootbeheersystemen, RFID-lezers, autonome magazijnrobots, industriële labelprinters, enz. Elk verbonden toestel vormt een potentieel toegangspunt als het niet correct beheerd wordt. Hoe meer toestellen, hoe groter het aanvalsoppervlak. Zo kan een onbeveiligde printer in een magazijn worden gehackt om picklijsten te saboteren, wat leveringen vertraagt. Het up-to-date houden en monitoren van deze niet-traditionele endpoints is dus cruciaal.

5. **Beperkte IT-staf en focus op kostenbesparing**
Traditioneel hebben veel logistieke bedrijven ingezet op efficiëntie en kostenreductie, vaak ten koste van IT-investeringen. Cybersecurity stond niet bovenaan de prioriteitenlijst. Door de NIS2-verplichtingen (en toenemende dreigingen) moeten ze nu snel hun capaciteiten uitbreiden. Tegelijk zijn de IT-teams vaak klein en moeten ze meer doen met dezelfde middelen. Automatisering en doeltreffende tools zijn noodzakelijk om deze kloof te overbruggen.

6. **Realtime gegevensbeveiliging**
Realtime gegevensuitwisseling is cruciaal (bv. live GPS-tracking, elektronische leveringsbewijzen, actuele voorraadupdates). NIS2 vereist dat deze datastromen beveiligd worden om vertrouwelijkheid en integriteit te garanderen. Toestellen moeten versleuteling en sterke authenticatie gebruiken en beschermd zijn tegen afluisteren of manipulatie. De uitdaging is om deze beveiliging onzichtbaar te maken voor de gebruiker – chauffeurs mogen geen IT-experts moeten zijn om veilig verbinding te maken.

7. **Menselijke fouten en bewustwording**
Net als andere medewerkers kunnen chauffeurs en magazijniers slachtoffer worden van phishing of onveilig gedrag vertonen (zoals het installeren van een game met malware). NIS2 benadrukt het belang van regelmatige opleiding en digitale hygiëne. In de praktijk moeten bedrijven manieren vinden om hun verspreid personeelsbestand continu op te leiden in beveiligingspraktijken – en indien nodig bepaald gedrag technologisch afdwingen (bv. het blokkeren van risicovolle websites op bedrijfsapparaten).

SOTI

SOTI-oplossingen voor logistiek: Endpoints beveiligen, compliance garanderen

Gecentraliseerd en schaalbaar apparaatbeheer

Of u nu 100 of 100.000 toestellen beheert, SOTI MobiControl schaalt moeiteloos mee. Het is zo krachtig en gebruiksvriendelijk dat één IT-medewerker wereldwijd meer dan 100.000 Android-apparaten kan beheren. Voor logistieke operaties die verspreid zijn over meerdere locaties is deze centralisatie een echte gamechanger. Vanuit het hoofdkantoor kan IT op afstand de configuratie en beveiliging beheren van elke robuuste scanner, boordtablet of mobiele computer in het veld. Het platform ondersteunt Android, iOS, Windows en Linux – ideaal voor de diversiteit aan apparaten in transportomgevingen. Dankzij functies zoals Express Enrollment kunnen nieuwe apparaten in enkele minuten uitgerold worden: rechtstreeks geleverd op de locatie en automatisch geconfigureerd bij het opstarten. Zo verlopen implementaties sneller, veiliger en zonder dat IT fysiek aanwezig moet zijn. Bovendien zorgt centrale controle ervoor dat alle toestellen dezelfde beveiligingsregels volgen – een vereiste voor NIS2-naleving. Geen enkel apparaat ontsnapt aan het beleid.

Realtime zichtbaarheid en gezondheidsmonitoring van toestellen

SOTI MobiControl biedt diepgaand inzicht in de status van elk apparaat: u ziet waar het zich bevindt (via GPS), welke apps actief zijn, het batterij- en geheugenniveau, en of er beveiligings- of complianceproblemen zijn. Als een handheld van een chauffeur zich abnormaal begint te gedragen (mogelijk door malware of een technisch defect), krijgt IT een waarschuwing. Het dashboard signaleert ook toestellen die offline zijn of geen verbinding maken, zodat proactief kan worden ingegrepen. Deze zichtbaarheid geldt ook voor IoT-apparaten via SOTI Connect – zoals het monitoren van printers of sensoren in het magazijn. Dankzij deze “vinger aan de pols” kunnen bedrijven kleine problemen oplossen vóór ze grote storingen veroorzaken. En wanneer auditors bewijs vragen van monitoring, toont u hiermee uw actieve risicobeheer.

Remote troubleshooting en zero-touch ondersteuning

In de logistiek is het vaak onmogelijk om defecte toestellen terug te sturen naar het hoofdkantoor – dat kost tijd, geld én verstoort het werk. Met de Remote Control functie van SOTI MobiControl kan IT het scherm van een toestel op afstand overnemen, instellingen wijzigen of updates pushen. Zo kan een chauffeur met een tabletprobleem onderweg rechtstreeks geholpen worden – zonder dat hij hoeft te stoppen. Eén klant rapporteerde dat problemen die vroeger “meerdere dagen productiviteitsverlies” veroorzaakten nu onmiddellijk op afstand worden opgelost. Minder downtime betekent stiptere leveringen – en een betere score op NIS2-vereisten rond incidentrespons en bedrijfscontinuïteit.

Sterke beveiliging en compliance-functionaliteiten

SOTI MobiControl bevat tal van beveiligingsmechanismen: authenticatie via pincode of biometrie, gegevensversleuteling, en functies zoals geofencing (waarbij een toestel alleen werkt binnen een bepaalde locatie, bv. binnen het magazijn). De Kiosk Mode is ideaal voor de sector: toestellen worden beperkt tot goedgekeurde apps, zoals dispatchingsoftware, navigatie en communicatie – niets anders. Dit voorkomt afleiding én beschermt gevoelige data tegen ongeoorloofde apps of downloads. Beveiligingsupdates en OS-patches kunnen automatisch op alle toestellen uitgerold worden op geplande tijdstippen – zonder de werking te storen. Zo blijft het volledige toestelpark gestandaardiseerd en “gehard”, wat essentieel is voor NIS2-naleving.

Veilig beheer van content en applicaties

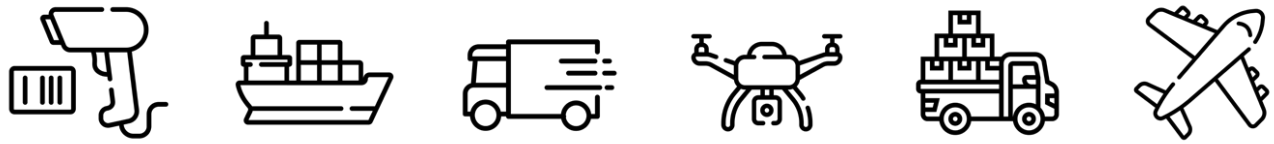
Logistiek personeel heeft vaak documenten of apps nodig onderweg – bv. douaneformulieren of interne tools. SOTI laat toe om deze content veilig te distribueren, zodat ze enkel toegankelijk is binnen een beveiligde omgeving op toegelaten apparaten. Ook apps kunnen centraal beheerd worden – installaties, updates en verwijderingen kunnen op afstand en in bulk gebeuren. Zo sluit u snel kwetsbare apps af en rolt u nieuwe software veilig uit. Dit ondersteunt ook compliance: als een app end-of-life is of in strijd is met beleid, kan SOTI garanderen dat ze overal verwijderd wordt.

IoT- en printerbeveiliging via SOTI Connect

In logistieke hubs zijn industriële printers, slimme transportbanden en sensoren dagelijkse realiteit. SOTI Connect centraliseert het beheer van deze IoT-apparaten – ongeacht merk of locatie. IT kan nieuwe printers uitrollen met standaardinstellingen, gebruik monitoren (aantal labels, foutmeldingen) en zelfs firmware-updates op afstand uitvoeren. Dit voorkomt dat vergeten apparaten – zoals printers – zwakke plekken worden in de beveiliging. SOTI kan zelfs meldingen sturen als een printer wordt verplaatst of gemanipuleerd. Onder NIS2, dat ook OT-systemen omvat, is dit een belangrijk pluspunt.

Analytics en optimalisatie van ROI

Een extra troef is SOTI XSight, dat toesteldata analyseert voor terugkerende problemen of prestatieknelpunten. Zo kan bijvoorbeeld aan het licht komen dat een bepaald type scanner vaker faalt in één magazijn – informatie die u helpt om downtime te voorkomen. Goed functionerende toestellen verhogen de productiviteit én versterken indirect de veiligheid (minder schaduw-IT of risicovol gedrag). Eén logistiek bedrijf in het VK bespaarde dankzij SOTI meer dan £250.000 per jaar – door kortere installatieperiodes, minder transportkosten en minder IT-uren. Deze besparingen kunnen opnieuw geïnvesteerd worden in beveiliging of innovatie.



Succesverhalen in Transport & Logistiek

Een grote bezorgdienst toont hoe gecentraliseerd mobiliteitsbeheer leidt tot zowel beveiliging als efficiëntie.

Onze klant is actief in meerdere Europese landen en voorziet chauffeurs van Android-handhelds voor het scannen van pakketten en routebeheer. In depots worden tablet-kiosken gebruikt voor voorraadopvolging. Voor de implementatie van SOTI was het IT-team overweldigd door het manueel beheren van duizenden toestellen. Instellingen waren vaak inconsistent; sommige chauffeurs stelden updates uit of installeerden ongeoorloofde apps (zoals sociale media), wat leidde tot beveiligingslekken en zelfs malware-infecties. Als een toestel defect raakte, moest het naar het hoofdkantoor worden teruggestuurd – een proces dat dagen duurde, waarbij de chauffeur intussen moest werken met een reserveapparaat of papieren procedures.

Sinds de invoering van SOTI MobiControl is alles veranderd.

Het IT-team beheert nu het volledige apparaatpark wereldwijd vanuit één centrale console. Elk toestel volgt automatisch de beveiligingsrichtlijnen via vooraf ingestelde profielen. Als een chauffeur probeert een beveiligingsinstelling uit te schakelen, zal SOTI deze onmiddellijk herstellen of IT waarschuwen.

Toestellen die offline raken of tekenen van inbraak vertonen, worden direct gesignaleerd. Volgens de IT-manager van de klant is het werk dat vroeger een heel team vereiste nu grotendeels geautomatiseerd – één beheerder kan vandaag alleen instaan voor meer dan 5.000 toestellen. Dat is enkel mogelijk dankzij SOTI's krachtige automatisering (vergelijkbaar met wat Delivery Hero realiseerde in een gelijkaardige context). Daardoor konden teamleden zich richten op proactieve verbeterprojecten in plaats van dagelijkse toestelproblemen.

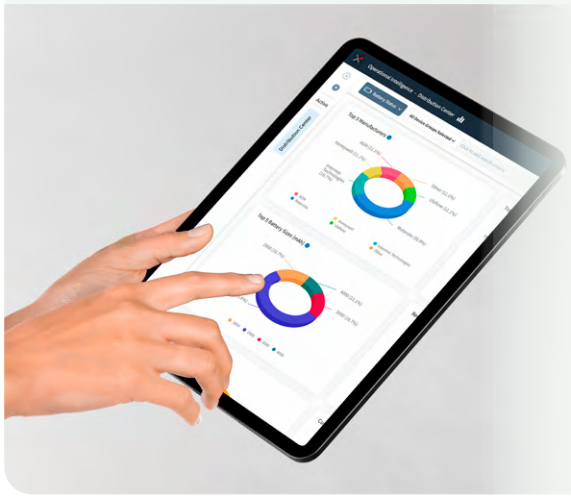
Daarnaast werd SOTI Snap ingezet om compliance en opleiding te versterken.

Men ontwikkelde een eenvoudige mobiele app voor chauffeurs met korte cybersecuritymodules en quizzen – over o.a. phishingherkenning of correct toestelgebruik. Via SOTI Snap werd de training automatisch en periodiek aangeboden op elk toestel, en centraal opgevolgd. Dit verhoogde de deelname aan cybersecurity-awareness aanzienlijk zonder dat chauffeurs klaslokaaltraining nodig hadden. De HR-afdeling kon de inhoud snel aanpassen en opnieuw verspreiden via het platform – snel, schaalbaar en traceerbaar.

Een ander succesverhaal komt van een Nederlands logistiek bedrijf («Fleetoran») gespecialiseerd in bouwmaterialentransport.

Fleetoran kampte met een wildgroei aan persoonlijke toestellen bij chauffeurs, met uiteenlopende appversies en zwakke beveiliging. Bovendien moesten er een twintigtal apps handmatig worden geïnstalleerd per toestel – wat bijna 30 minuten duurde.

Na de invoering van SOTI MobiControl en het uitrollen van bedrijfstoestellen, daalde de configuratietijd tot minder dan 5 minuten per toestel – een tijdsbesparing van meer dan 80%.



Dankzij automatische profielen worden alle noodzakelijke apps en instellingen bij inschrijving meteen toegepast. Deze efficiëntiewinst leverde jaarlijks meer dan €250.000 op, door lagere IT-kosten en minder overuren.

Ook de beveiliging ging erop vooruit:

Dankzij de Kiosk Mode kregen chauffeurs enkel toegang tot essentiële apps, en via Remote Control kon IT snel tussenkomen bij problemen. Fleetoran elimineerde vrijwel alle vertragingen die vroeger ontstonden bij toestelproblemen die teruggestuurd moesten worden. Een SOTI-vertegenwoordiger benadrukte dat het bedrijf nu «problemen op afstand kan oplossen, toestellen en apps tegen externe bedreigingen beveiligt en altijd up-to-date blijft met compliance-eisen» – precies wat nodig is om te voldoen aan NIS2.

Vandaag starten de chauffeurs hun werkdag met betrouwbare, veilige tools, terwijl het management gerust is dankzij zichtbaarheid en controle over het hele toestelpark. Problemen worden vroegtijdig opgespoord – nog voor ze schade kunnen aanrichten.

Kortom: SOTI transformeert toestelbeheer van een operationele last naar een strategisch voordeel.

Bedrijven voldoen niet alleen aan de compliance-eisen (met documenteerbare controles, auditlogs en trainingen), maar realiseren ook kostenbesparingen en productiviteitswinsten.

De weg naar NIS2-naleving wordt zo meer dan een wettelijke verplichting – het is een kans om te moderniseren en efficiënter te werken.

Conclusie en volgende stappen voor logistieke besluitvormers

De boodschap is duidelijk: cybersecurity is vandaag net zo essentieel voor transport en logistiek als brandstof voor de vrachtwagen of software voor het magazijn. De NIS2-richtlijn versnelt een mentaliteitswijziging in de sector: beveiliging en compliance zijn niet langer louter IT-zaken, maar vormen de kern van bedrijfscontinuïteit en betrouwbare dienstverlening.

Deze white paper toont aan dat u met de juiste tools – in het bijzonder een krachtig platform voor mobiel en endpointbeheer – niet hoeft te kiezen tussen veiligheid en efficiëntie.

SOTI MobiControl en het SOTI ONE Platform combineren beide aspecten: ze geven uw compacte IT-team de mogelijkheid om een grote, verspreide vloot van apparaten te beheren met ongeziene controle en automatisering, én verbeteren tegelijk de gebruikerservaring van uw medewerkers in het veld (zoals chauffeurs en magazijniers).

In het kader van NIS2 biedt SOTI de technische middelen om veel van de verplichte maatregelen te implementeren – zoals activabeheer, toegangscontrole, incidentrespons en continue monitoring – in één geïntegreerde oplossing.

Het resultaat is een logistieke operatie die cyberweerbaar is (in staat om aanvallen te weerstaan en snel te herstellen) en van nature compliant, zonder dat de dagelijkse leveringen eronder lijden.

Bedrijven actief in vrachtvervoer, spoor, luchtvracht of warehousing rapporteren concrete voordelen dankzij SOTI:

- drastisch minder toesteluitval
- aanzienlijke besparingen op IT- en supportkosten
- én meer vertrouwen van klanten en partners in de beveiliging van hun diensten.

Dit alles vertaalt zich in een concurrentievoordeel: wie nu al investeert in compliance en beveiliging, wint het vertrouwen én mogelijk marktaandeel ten opzichte van wie achterop blijft.

Er is ook gemoedsrust: een verloren toestel leidt niet tot een datalek in de media, en een cyberincident wordt meteen ingedamd dankzij de juiste tools.

Tijd voor actie

De NIS2-deadlines komen dichterbij en cyberdreigingen blijven evolueren.
Het beveiligen van uw mobiele operatie en voldoen aan NIS2 zou bovenaan uw agenda voor 2025 moeten staan.

HET GOEDE NIEUWS? U HOEFT DIT TRAJECT NIET ALLEEN AF TE LEGGEN.

Volgende stappen

1. Boek een demo
Zie SOTI MobiControl in actie tijdens een live demonstratie op maat van uw logistieke realiteit.
Bekijk hoe eenvoudig het is om een toestel te lokaliseren, software bij te werken of een probleem op afstand op te lossen. Seeing is believing.

2. Vraag een NIS2-compliancecheck aan
Onze SOTI-experts voeren een korte review uit van uw huidige apparaatbeheer en identificeren eventuele gaten t.o.v. de NIS2-verplichtingen.
U ontvangt best practices en een concreet stappenplan – als een “cybergezondheidscheck” met meteen bruikbare inzichten.

Tot slot

Naleving van NIS2 draait niet alleen om het vermijden van boetes of voldoen aan een wetgeving.

Het is een kans om uw logistiek te versterken, slimmer te maken en toekomstbestendig te bouwen.

Door het SOTI ONE Platform te benutten, maakt u van uw toestelpark een concurrentievoordeel: hoogbeveiligd, geïntegreerd en betrouwbaar – dag in dag uit.

Neem vandaag nog contact op met eutronix om deze reis te starten.

LATEN WE SAMEN ZORGEN DAT UW TRUCKS EN PAKKETTEN SNEL BLIJVEN BEWEGEN – TERWIJL UW CYBERSECURITY ROTSVAST BLIJFT.

www.eutronix.eu

Is uw toeleveringsketen echt op de hoogte van de NIS2-vereisten?

Laat compliance niet verworden tot een simpele inhaalslag: door nu te anticiperen verandert u een wettelijke beperking in een stimulans voor efficiëntie en vertrouwen voor al uw activiteiten.
Door gebruik te maken van de gezamenlijke expertise van eutronix en SOTI kunt u uw mobiele terminals beveiligen, uw gegevensstromen stroomlijnen en de servicecontinuïteit garanderen die uw klanten verwachten.

Neem vandaag nog contact op met onze experts.
We bespreken graag met u hoe we onze oplossing kunnen afstemmen op uw specifieke behoeften.

eutronix België
1300 - Wavre

+32 10 39 49 00

Contact opnemen

eutronix Frankrijk
78870 - Bailly

+33 1 34 61 61 46

Contact opnemen

eutronix Nederland
4744 RZ Bosschenhoofd

+31 76 52 45 330

Contact opnemen

Over eutronix

- Een dynamisch bedrijf dat zich specialiseert in hardwareoplossingen en elektronische automatiseringsapparatuur
- Value-added distributor
- Opgericht in 1999
- Hoofdkantoor in België
- Vestigingen of dochterondernemingen in Frankrijk, Nederland en het Verenigd Koninkrijk
- Een team van meer dan 40 mensen

eutronix' sectoren

- Gezondheidszorg
- Horeca
- Retail
- Vrijetijdssector
- Transport & logistiek
- Industrie
- Toegangscontrole
- Signalering
- Field service
- Oem & IoT