

PASSANT^{2.0}



Aanleiding:

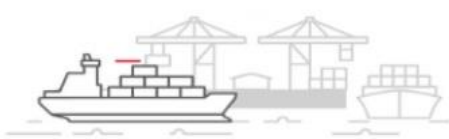
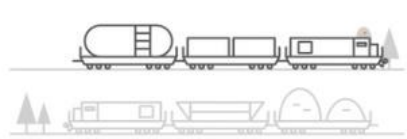
Gedurende het project PASSANT signaleerde de diverse partners dat er vanuit de havens c.q. logistieke sector een behoefte bestaat aan ondersteuning in de strijd tegen criminaliteit. Vooral vanuit economisch, publicitair en maatschappelijk perspectief is de concrete wil om ondermijning / criminaliteit te weren. Hiervoor is reeds een grote zoektocht gaande naar de juiste in te zetten middelen. Uit de vraagarticulatie in de sector blijkt de noodzaak aan duidelijke criminaliteit werende richtinggevende maatregelen; “Wat moet ik doen, wat werkt wel/niet, wat zijn de kosten, wat is effectief, hoe behaal ik het meeste effect, is er reeds ervaring hiermee in dezelfde sector, wat is de schaalbaarheid, ... ?”

Vanuit de wens om te innoveren is het belangrijk dat de vraag uit de markt in het juiste perspectief wordt belicht. In het project PASSANT hebben we hiertoe een leidraad ontwikkeld in een veiligheid/beveiliging maatregelen dashboard voor de diverse hubs in de logistieke sector. Enerzijds een handreiking voor de beveiliging van de eigen logistiek hub anderzijds een verbindend middel om ervaringen uit te wisselen en vraag en aanbod met betrekking tot innovaties te duiden.

Het dashboard kan dienen als het fundament van een kennisbank van oplossingen in de strijd tegen criminaliteit.

Op de volgende pagina's de uitwerking hiervan,

PASSANT team *Coördinatoren Jan Otten & Vincent Leroy* - contact@passant.info

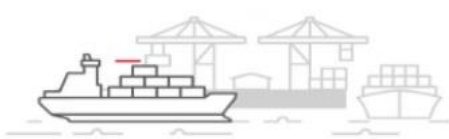
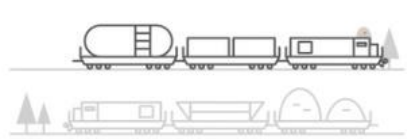


Richtinggevende maatregelen voor logistieke hubs

preventief en proactief tegen criminaliteit

(ondermijning en high impact crime)





6 Maatregel-dashboards voor criminaliteitspreventie

Fysiek

F.1

Sluit onbevoegden buiten en bewaak je eigendom

F.2

Verscherp fysiek en virtueel toelatingsbeleid (ook cyber)

F.3

Zet bewezen en gecertificeerde technologische middelen in

F - Fysiek

Maatregelen om onbevoegden (ook virtueel) te weren

F.1 Sluit buiten

- Omheining – hekken, grachten
- Netwerk / endpoint security

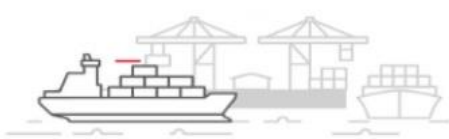
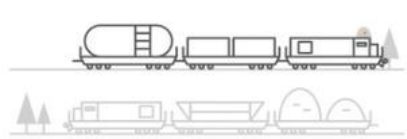
F.2 Scherpe toegangscontrole

- Controleer personeel en bezoekers
- Tref diverse cyberbeveiligingen (wachtwoorden, e-mail security, vpn, firewall, ...)

F.3 Gebruik bewezen technologieën

- Leer van anderen die producten reeds in praktijk inzetten (best practices)
- Schaf gecertificeerde producten / technologieën aan





6 Maatregel-dashboards voor criminaliteitspreventie

Detectie

D.1

Plaats en gebruik meerdere sensoren (beeld, geluid, geur,..)

D.2

Leer en herken afwijkende patronen (automatisch)

D.3

Creër continu beeld (mapping, UAV's)

D - Detectie

Maatregelen om onbevoegden te signaleren

D.1 Zet sensoren in

- Camera's, trillingen, geur, geluid, drones, ...
- Verbind de sensoren

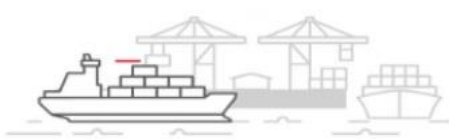
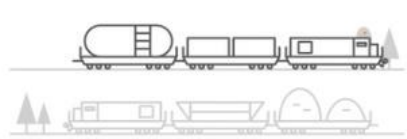
D.2 Leer en herken

- Herken afwijkende patronen
- Leer normaal van abnormaal te onderscheiden

D.3 Zorg voor continu beeld

- Verschaf continu zicht met de vaste sensoren
- Gebruik extra sensoren om situatieanalyse verbeteringen





6 Maatregel-dashboards voor criminaliteitspreventie

Informatie

I.1

Vergelijk logistieke planning en data met wat er echt gebeurt

I.2

Analyseer open en gesloten data ook in periferie (buiten)

I.3

Zoek algoritmes en pas kunstmatige intelligentie toe

I - Informatie

Maatregelen om signalen en werkelijkheid te matchen

I.1 Vergelijk continu

- Wat verwacht wordt volgens planning
- Wat de werkelijke situatie is / werkelijk gebeurt

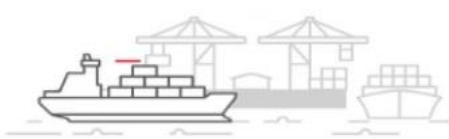
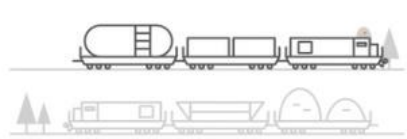
I.2 Analyseer

- Blijf op de hoogte via diverse informatie bronnen
- Onderzoek, pas aan en verbeter aan de hand van ontsloten informatie

I.3 Kunstmatige Intelligentie (AI)

- Maak gebruik van AI om sneller situaties bloot te leggen
- Stel algoritmes op voor de normale ICT huishouding





6 Maatregel-dashboards voor criminaliteitspreventie

Co creatie

C.1

Versterk netwerken en maak overeenkomsten met stakeholders

C.2

Maak afspraken over uitwisselen data, kennis en informatie

C.3

Stel protocollen en normenkaders ook bij escalatie

C – Co-creatie

Maatregelen om te verbinden en op de hoogte te blijven

C.1 Netwerk

- Zorg dat je alle stakeholders verbind
- Maak duidelijke afspraken over samenwerken

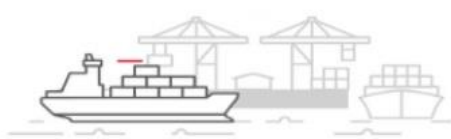
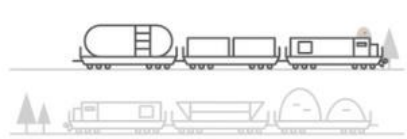
C.2 Data en informatie

- Maak afspraken en contracten over uitwisseling
- Wissel data, kennis en informatie uit

C.3 Escalatie

- Leg protocollen en plannen voor eventuele escalatie contractueel vast
- Volg protocollen en plannen voor eventuele escalatie





6 Maatregel-dashboards voor criminaliteitspreventie

Bewust

B.1

Werk aan bewustwording gedrag en cultuur

B.2

Design criminaliteit ontmoedigende technieken

B.3

Leid op, train, communiceer en dissemineer resultaten

B – Bewust

Maatregelen om bewust te werken aan integriteit en veiligheid

B.1 Beïnvloed

- Stel huisregels op ter bevordering van veilig gedrag
- Waarschuw voor gevolgen van onveilig gedrag

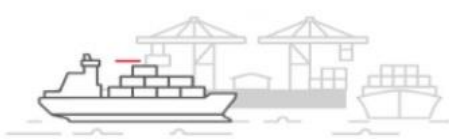
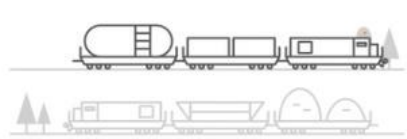
B.2 Design

- Ontmoedig criminaliteit 'by design' (bijv. via nudging, procedures of producten)
- Maak veiligheid sociaal gemeengoed

B.3 Train

- Maak personeel en bezoekers veiligheidsbewust door training en communicatie
- Dissemineer ervaringen en resultaten





6 Maatregel-dashboards voor criminaliteitspreventie

Actief

A.1

Verbind en bouw
Overzicht-Inzicht –
Draagvlak >
zorg voor impact

A.2

Observeer, Oriënteer,
Beslis
en Acteer
(steeds opnieuw)

A.3

Controleer, evalueer
en blijf aanjagen

A - Actief

Maatregelen om continue aandacht op veiligheid te zekeren

A.1 Draagvlak

- Geef overzicht en inzicht
- Werk aan draagvlak en impact

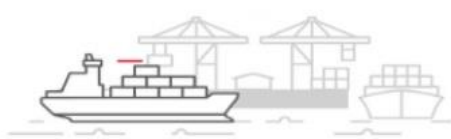
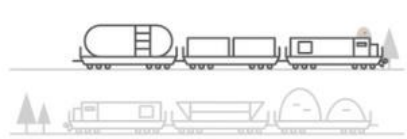
A.2 OODA loop

- Observeer > Oriënteer > Beslis (Decide) > Acteer
- Versnel proces (sneller dan crimineel)

A.3 Jaag aan

- Controleer en evalueer
- Stuur bij en jaag aan





6 Maatregel-dashboards voor criminaliteitspreventie



Fysiek

F.1
Sluit onbevoegden
buiten
en bewaak je
eigendom

F.2
Verscherp
fysiek en virtueel
toelatingsbeleid
(ook cyber)

F.3
Zet bewezen en
gecertificeerde
technologische
middelen in

Detectie

D.1
Plaats en gebruik
meerdere sensoren
(beeld, geluid, geur,
...)

D.2
Leer en herken
afwijkende
patronen
(automatisch)

D.3
Creëer continu
beeld (mapping,
UAV's)

Informatie

I.1
Vergelijk logistieke
planning en data
met wat er echt
gebeurd

I.2
Analyseer open en
gesloten data ook in
periferie (buiten)

I.3
Zoek algoritmes en
pas kunstmatige
intelligentie toe

Co creatie

C.1
Versterk netwerken
en maak
overeenkomsten
met stakeholders

C.2
Maak afspraken
over uitwisselen
data, kennis en
informatie

C.3
Stel duidelijke
protocollen en
normenkaders ook
bij escalatie

Bewust

B.1
Werk aan
veiligheids-
bewustwording
gedrag en cultuur

B.2
Design criminaliteit
ontmoedigende
technieken

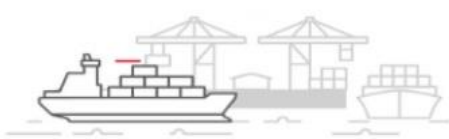
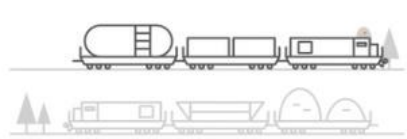
B.3
Leid op, train,
communiceer en
dissemineer
resultaten

Actief

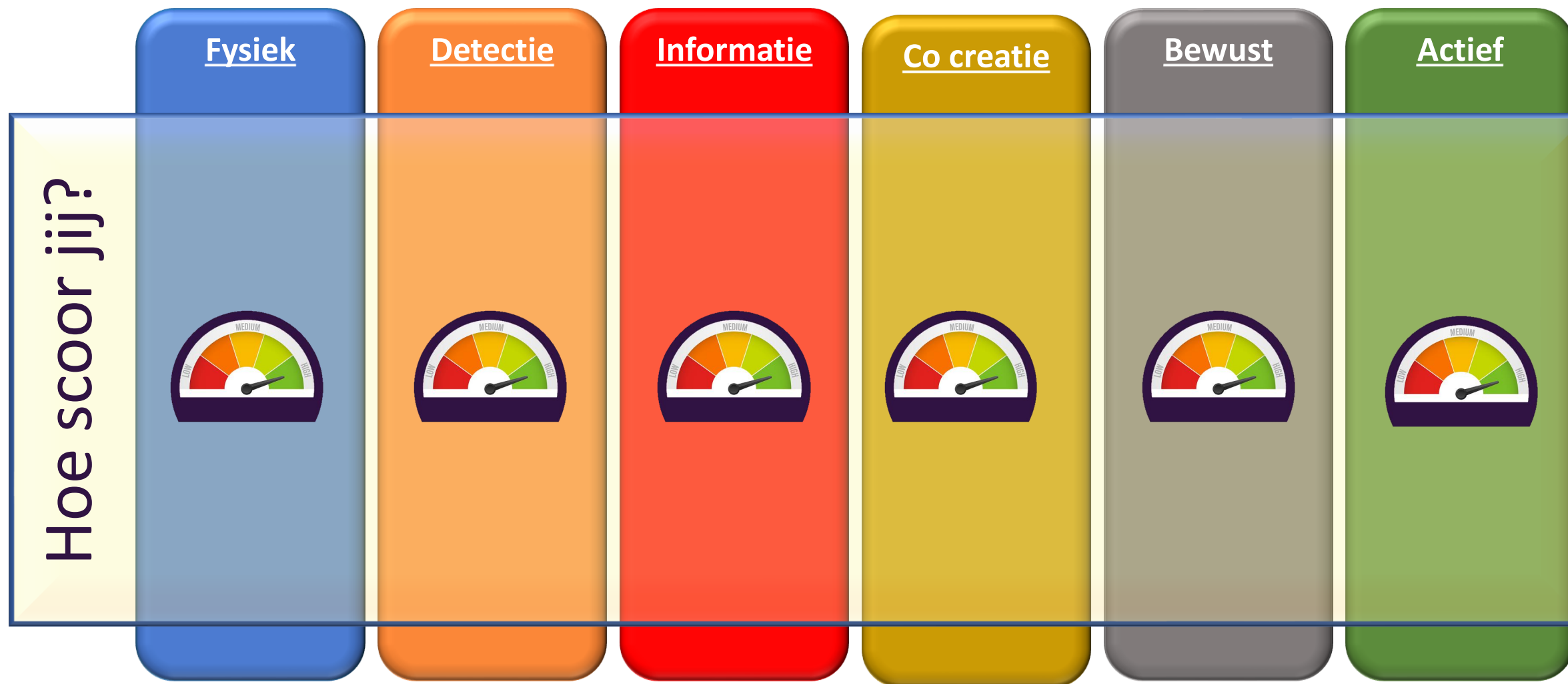
A.1
Verbind en bouw
Overzicht-Inzicht –
Draagvlak >
zorg voor impact

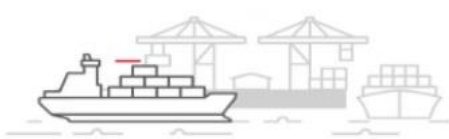
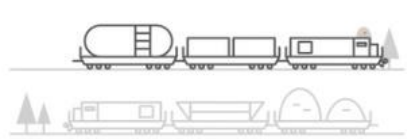
A.2
Observeer,
Oriënteer, Beslis
en Acteer
(steeds opnieuw)

A.3
Controleer, evalueer
en blijf aanjagen



Vraagarticulatie door reflectie van eigen logistieke hub op de 6 dashboards



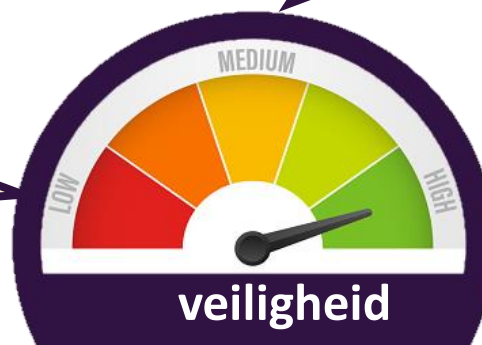


Samenwerken aan weerbare logistieke hubs

Handvat voor verbindende kennisbank van oplossende maatregelen

Handvat voor logistieke hubs in het weren van criminaliteit

Handvat voor regie op vraag en aanbod ten behoeve van innovaties in de strijd tegen criminaliteit



Info: contact@passant.info