Pilot netwerkdetectie rijksinternetvoorziening

Toelichting aan PRO/OOR

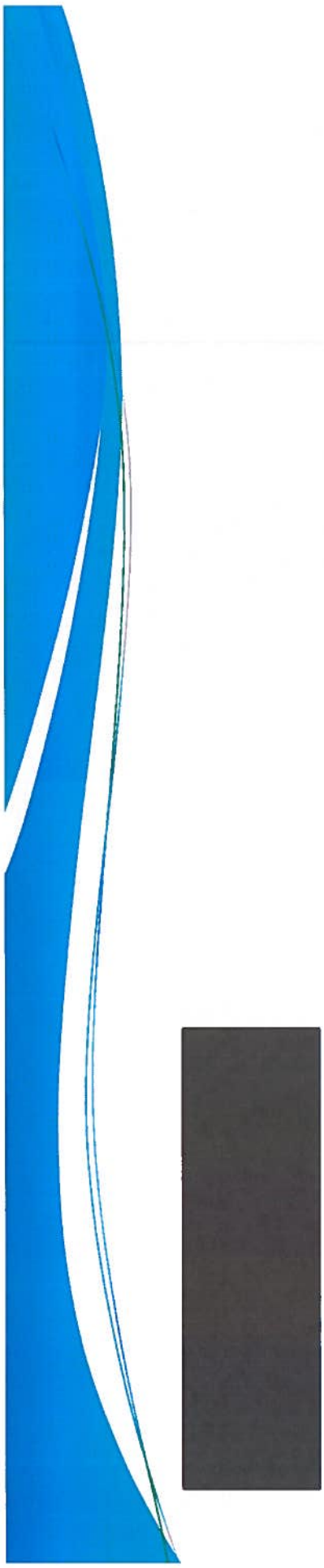
2 december 2013

Agenda

1. Aanleiding pilot
2. Opzet en bereik
3. Medezeggenschap
4. Werking
5. Vragen

Aanwezig

[redacted]



Aanleiding pilot

Nederland ICT land
- dekkingsgraad 94%
- hyperconnectiviteit
- toename cloud gebruik
- big data

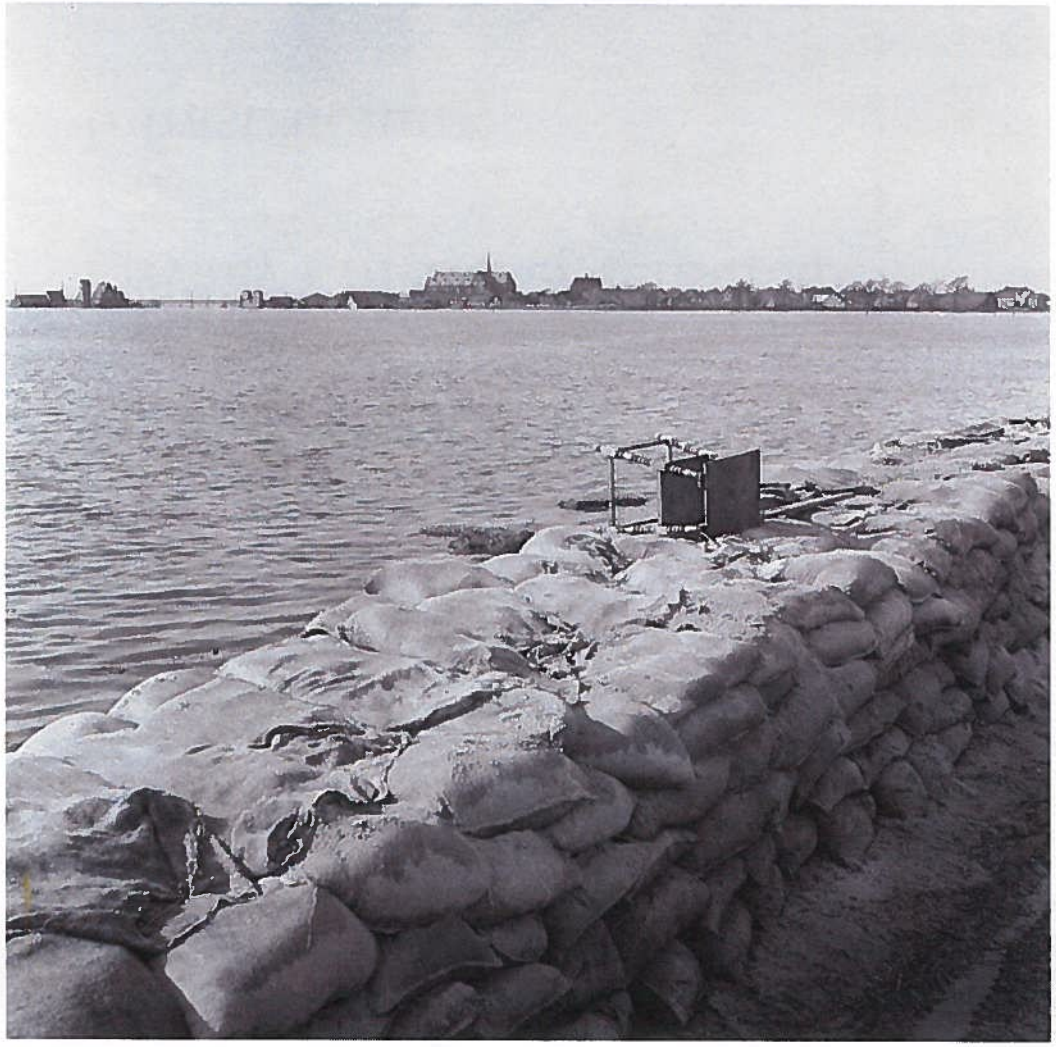
We zijn kwetsbaar
- 1.516 advisories
- business vs security
- kennis en middelen
- reputatie, vertrouwen

Toenemend misbruik
- spionage
- gerichte aanvallen
- meer unieke malware
- het wordt makkelijker

Aanleiding pilot

- Randvoorwaarden
- Ontsluiten van informatie
- Opbouw in 2014
- Samenwerking en pilot

Pilot opzet en bereik



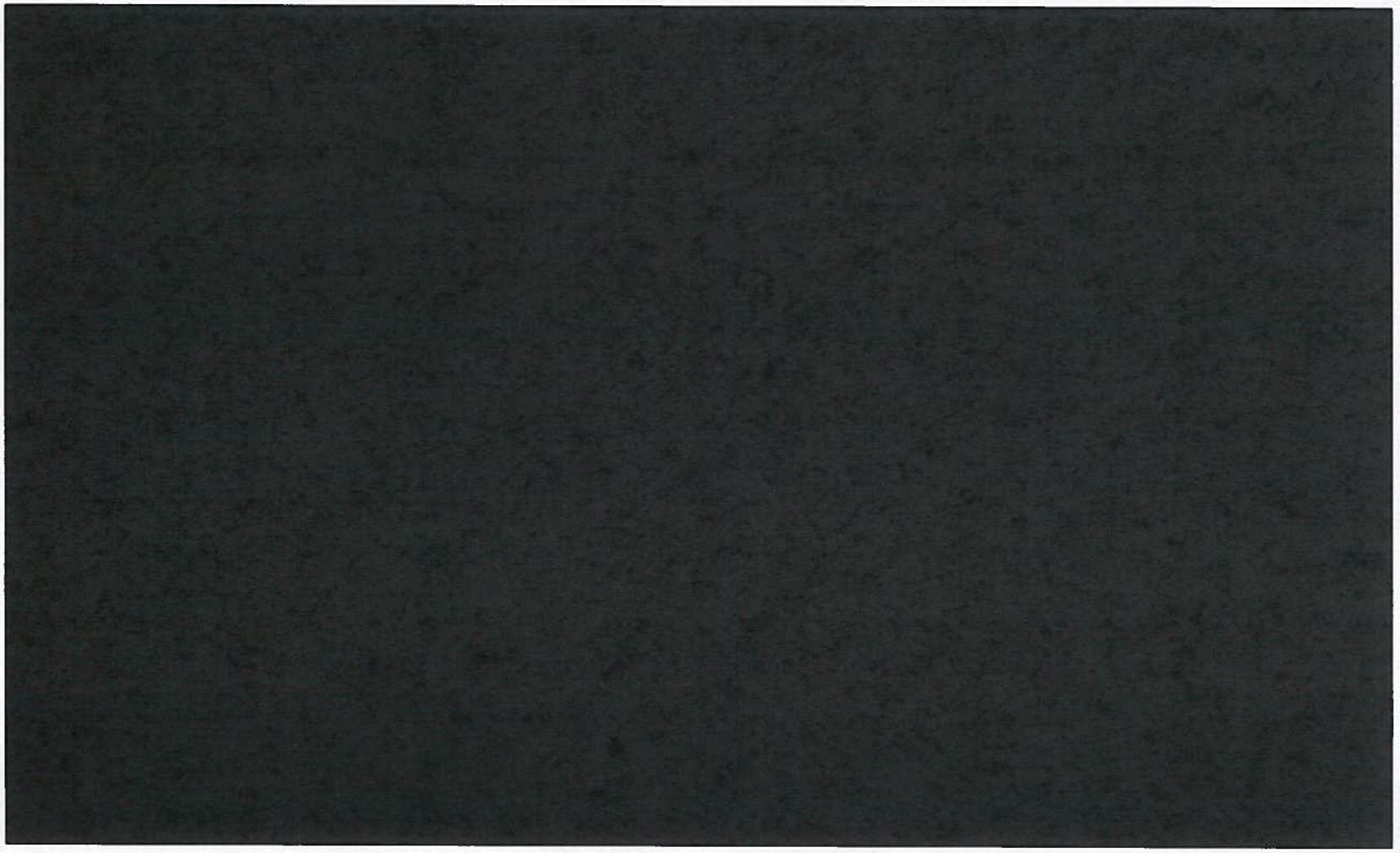
- SSC-ICT
- Bestaande situatie
- Doelen
- Start/eind

Pilot opzet en bereik

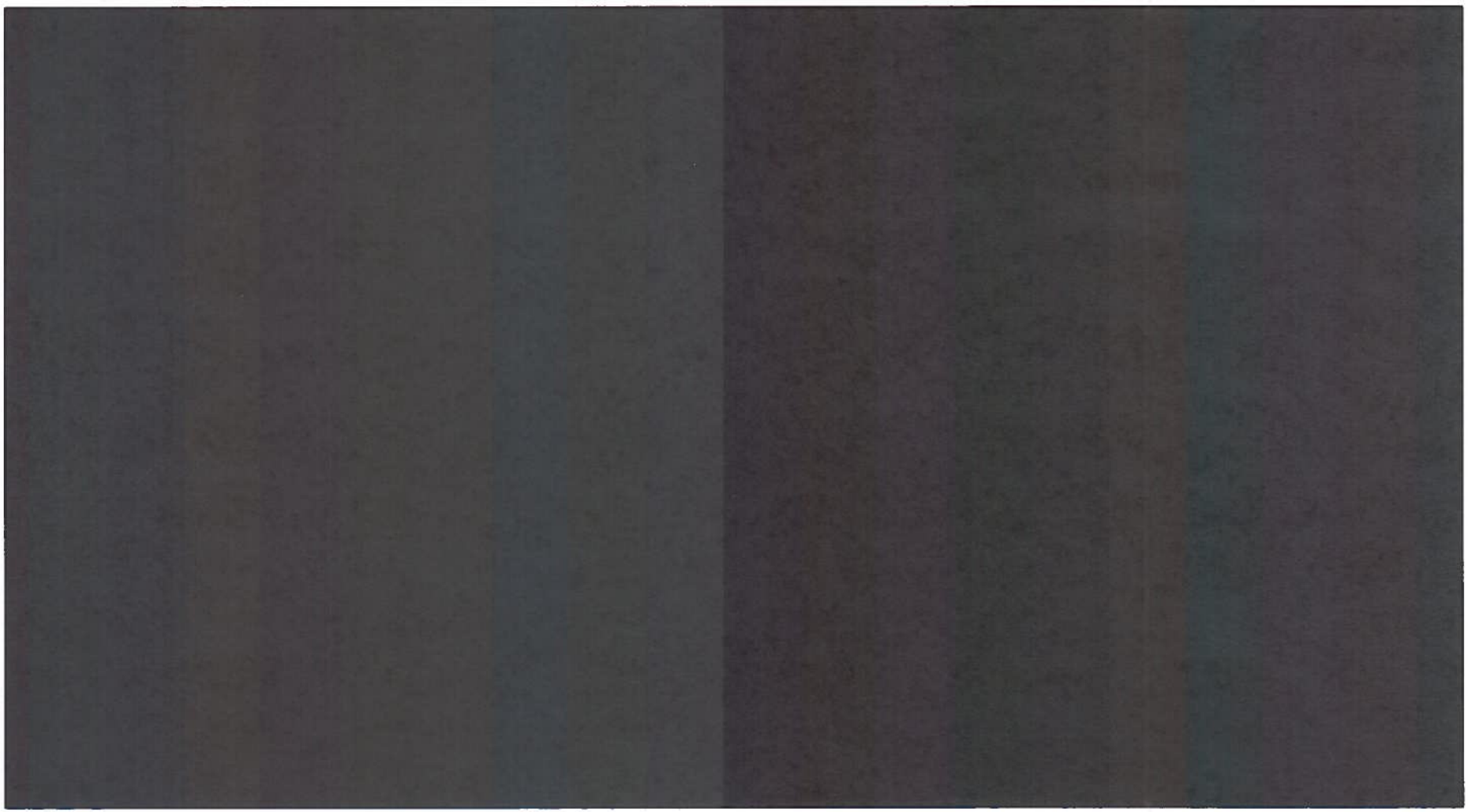
FASE I	FASE II	FASE III
Politiek / bestuurlijk	Voorbereiding pilot	Uitvoering pilot
Privacy / medezeggenschap		
Infrastructuur		
Systemen, processen, organisatie		

2013			2014	
mrt	nov/dec	dec	dec/jan	mei/jun

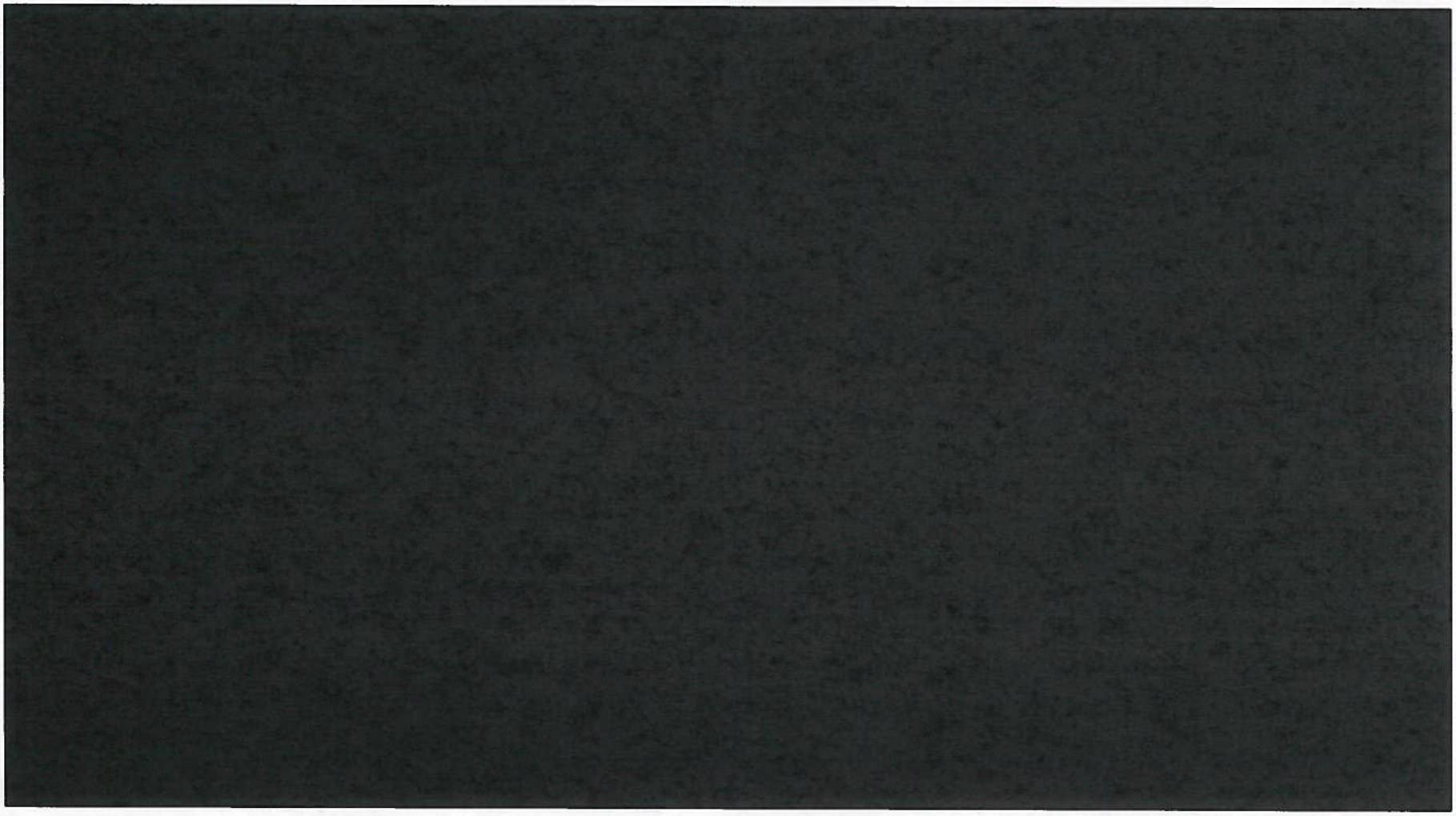
Opzet en bereik pilot



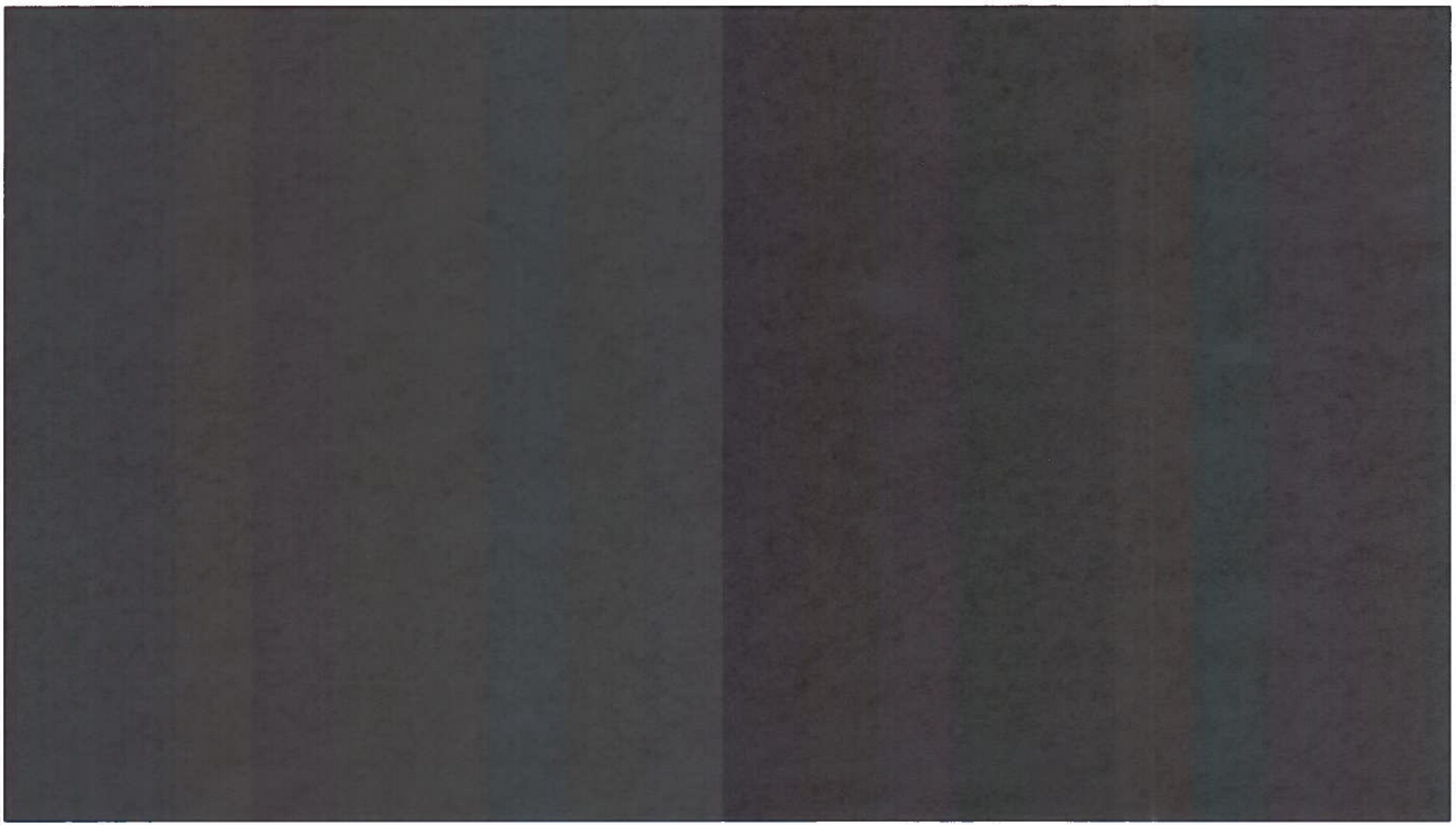
Opzet en bereik (fase II)



Opzet en bereik (fase II + III)

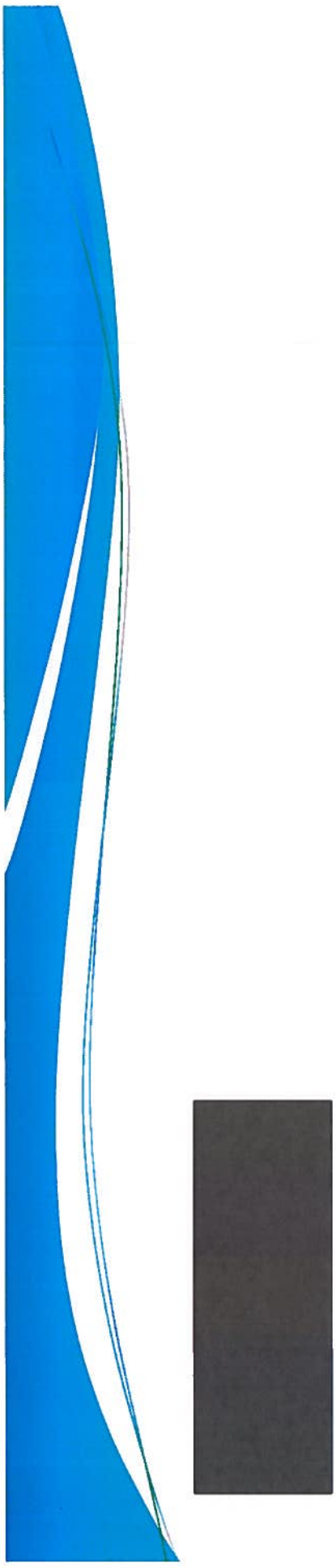


Opzet en bereik (fase II + III)



Medezeggenschap

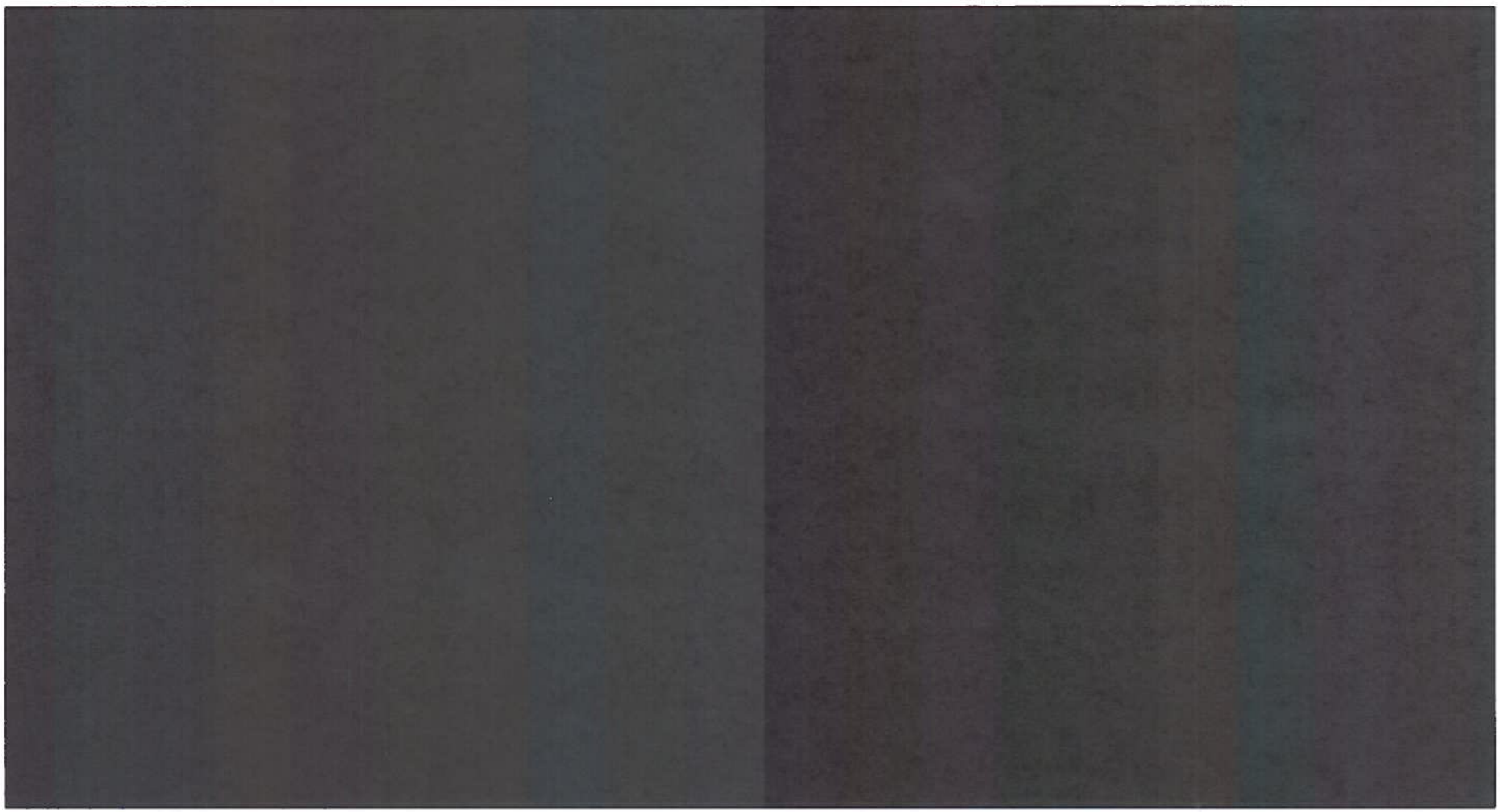
1. Focus op beveiliging netwerkverkeer
2. Toezicht en waarborgen
3. Transparant informeren
4. Data is en blijft bij SSC-ICT
5. Inzicht in events, niet in netwerkverkeer
6. OOR



Werking

- Landschap
- Input: signatures
- Output: events
- Procesoverzicht

Landschap

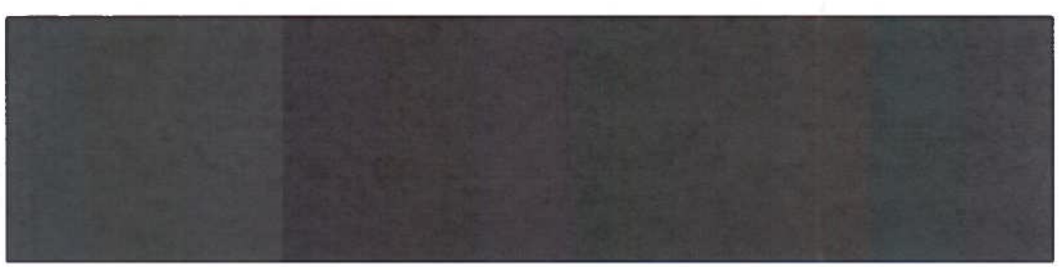


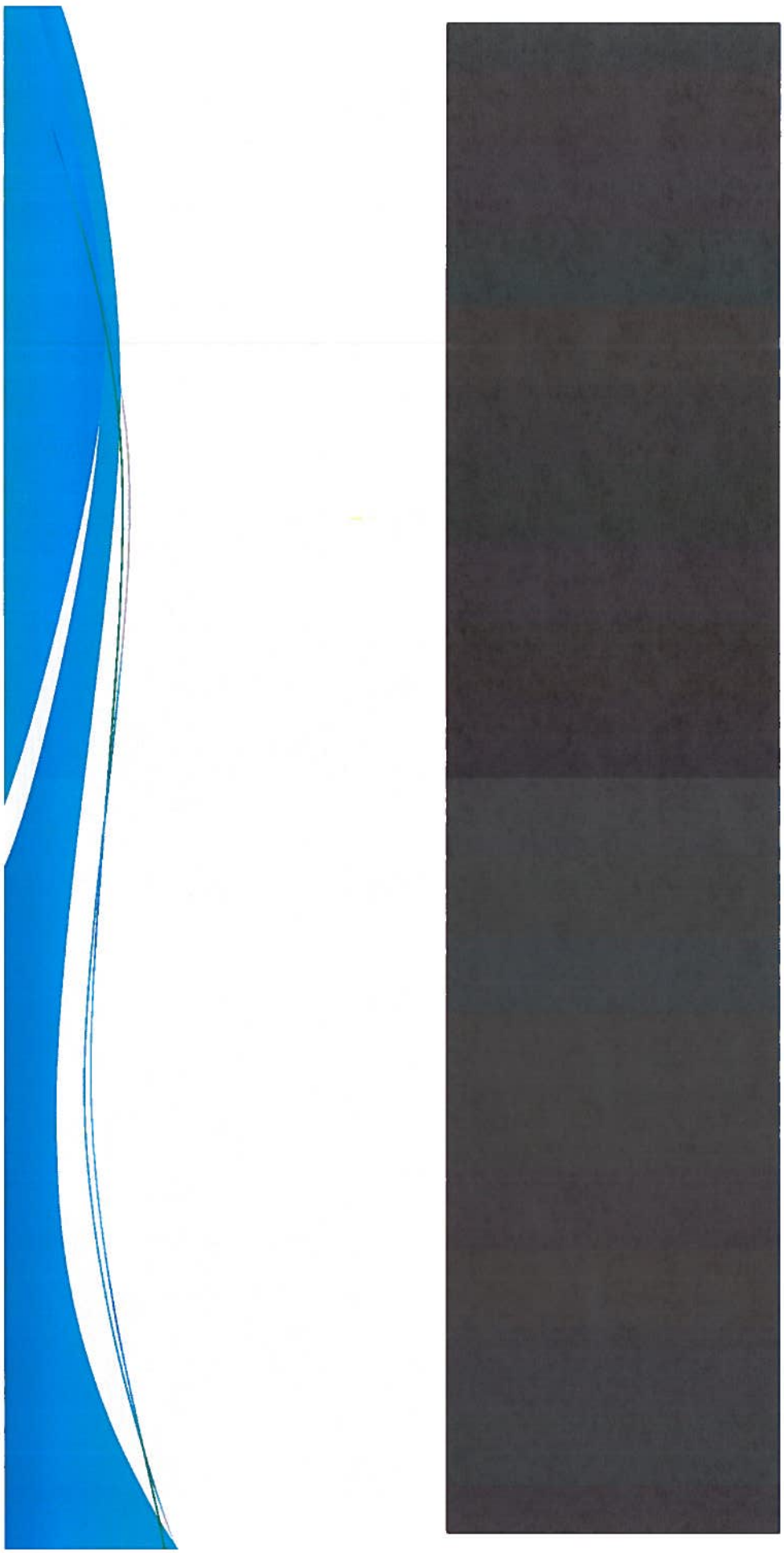
Input: signatures / patronen

- Input: signatures
- Opslag
- Type
- Kenmerken

Output: meldingen / events

Veldnaam	Omschrijving
Uniek bericht ID	Een uniek gegeven waarmee het alert bericht geïdentificeerd kan worden.
Detector ID	Samen met Detector locatie is dit een uniek gegeven waarmee de detector geïdentificeerd kan worden.
Detector Type	Het type detector, b.v. NCSC detector of 3rd party Detector
Detector Plugin Type	Het type plugin, b.v. DNS
Detector locatie	Samen met Detector ID is dit een uniek gegeven waarmee de detector geïdentificeerd kan worden.
Detect Time	Tijdstip waarop de detectie plaatsvond
Create Time	Tijdstip waarop het Alert is aangemaakt
Source IP	IP adres van het verzendende systeem
Source MAC	MAC adres van het verzendende systeem
Source Port	Poortnummer van het verzendende systeem
Source Protocol	Gebruikte protocol (TCP, UDP, ICMP) van het verzendende systeem
Destination IP	IP adres van het ontvangende systeem
Destination MAC	MAC adres van het ontvangende systeem
Destination Port	Poortnummer van het ontvangende systeem
Destination Protocol	Gebruikte protocol (TCP, UDP, ICMP) van het ontvangende systeem
Alert ID	Een uniek gegeven waarmee het type alert geïdentificeerd kan worden
DNS Query	De DNS zoekvraag, dit kan een domeinnaam zijn of een IP adres
DNS Response	Het antwoord, dit kan een domeinnaam zijn of een IP adres
RR Type	Het DNS record type, geeft aan wat voor antwoord het is. Dit kan IPv4, IPv6, Canonical Name of Nameserver zijn
TTL	De time-to-live geeft aan hoe lang een waarde wordt gecached in de DNS server

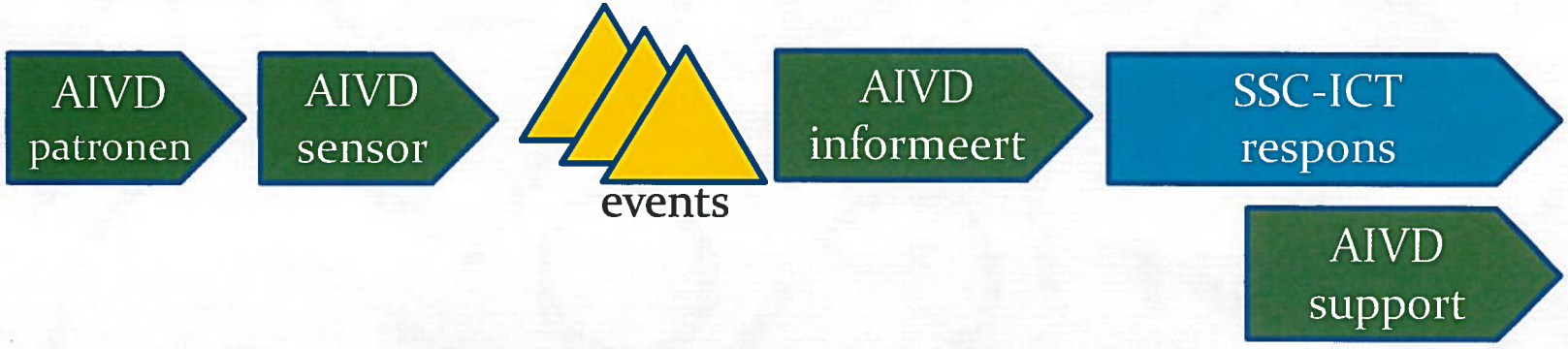




Procesoverzicht

DWR

RIJKSINTERNET




QUESTIONS

SINTERKLAAS JOURNAAL

Zaterdag 16 november 2013, jaargang 6, nummer 2 Bezorginformatie: www.sinterklaasjournaal.nl

Geen lied voor Luisterpiet

Luisterpiet was afgelopen tijd erg druk met luisteren en alles over ons op te schrijven voor Sinterklaas. Als er op scholen Sinterklaasliedjes worden gezongen, blijft hij altijd wat langer luisteren. Maar gisteren klonk er uit de schoorsteen van basisschool 'De Wegwijzer' geen enkel geluid. Toen Luisterpiet door het raam keek, zag hij dat 'De Wegwijzer' een school voor dove kinderen is, en die zingen in gebarentaal.