# LEVERINGSNETWERKEN

ANDRE SMULDERS

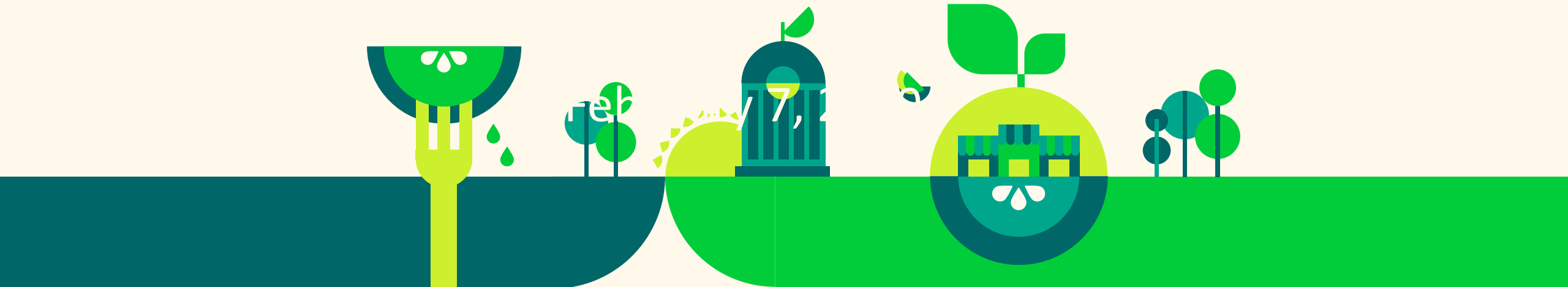
# KETENS EN NETWERKEN

# VERSCHILLENDE PERSPECTIEVEN


15
PvIB
reconnect
in cyber security

# Ahold Delhaize Information Security

PvIB Rondetafel: Supply Chain Cyber Risk



# Context van het project

- Ransomware @ Logistieke Partner
  - Distributiecentrum geïsoleerd
  - Geen leveringen meer aan Albert Heijn resulterend in lege schappen
  - Externe expertise nodig om de situatie onder controle te krijgen
  - Langdurige verstoring
- Observatie (1) : Cyber aanvallen op de supply chain zullen ongetwijfeld vaker optreden
  - Albert Heijn en leveranciers moeten maatregelen nemen om kans en impact te verminderen
- Observatie (2): Albert Heijn heeft verschillende belangrijke partners in de supply chain
  - Hoge afhankelijkheid van ongestoorde (dagelijkse) leveringen
- Belangrijke vragen
  - Hoe kwetsbaar is onze supply chain?
  - Hoe kunnen we risico's in de supply chain mitigeren?
  - Hoe moeten we reageren in vergelijkbare situaties?

# Doel van het project

## Opdracht

**Onze bescherming tegen aanvallen op onze partners:**

- **IT Security Assessment per supply chain partner**
- BCM Assessment per supply chain partner
- Bepaal de Juridische visie van  AH op vergelijkbare situaties
- Minimaliseer de impact op de klant
- Wees een betrouwbare partner

## Resultaat

**Onze bescherming tegen aanvallen op onze partners:**

- Levering van een IT Security assessment en een hierop gebaseerd security verbeterplan per supplier
  - Periodoeke bewaking van de voortgang
- Opname van security addendum in ALLE (incl. non-IT) supplier contracten.
  - Ondersteuning van de partners met basis requirements.
- Vorming van een supplier community om ondersteuning te geven en kennis te delen
  - Accountability en verantwoordelijkheid ligt bij de supplier
- BCM verbeterplan per supplier
- Verzorg runbooks voor het opzetten van (ad-hoc) leveringen voor het geval de IT is uitgevallen

# Kritische Succes Factoren

- **Duidelijke verwachtingen van senior management:**
  - Directeur AH strategic sourcing neemt de leiding en bepaalt de prioriteit van de in scope suppliers
  - In- en externe communcatie, focus op samenwerking en win-win
  - Verschillende disciplines in AH werken nauw samen: Sourcing, IT, BCM, Information Security

- **Ondersteuning van senior management aan de kant van de supplier:**
  - Directe betrokkenheid van supplier senior management.
  - Eenvoudige toegang tot supplier SMEs bij het uitvoeren van risk assessments
  - Risico rapportages gaan ook naar supplier senior management

- **Supplier SME validatie van bevindingen:**
  - Validatie van bevindingen door supplier SMEs met als doel een gedragen vastlegging van risico's te verkrijgen vóórdat er formele rapportage plaatsvindt

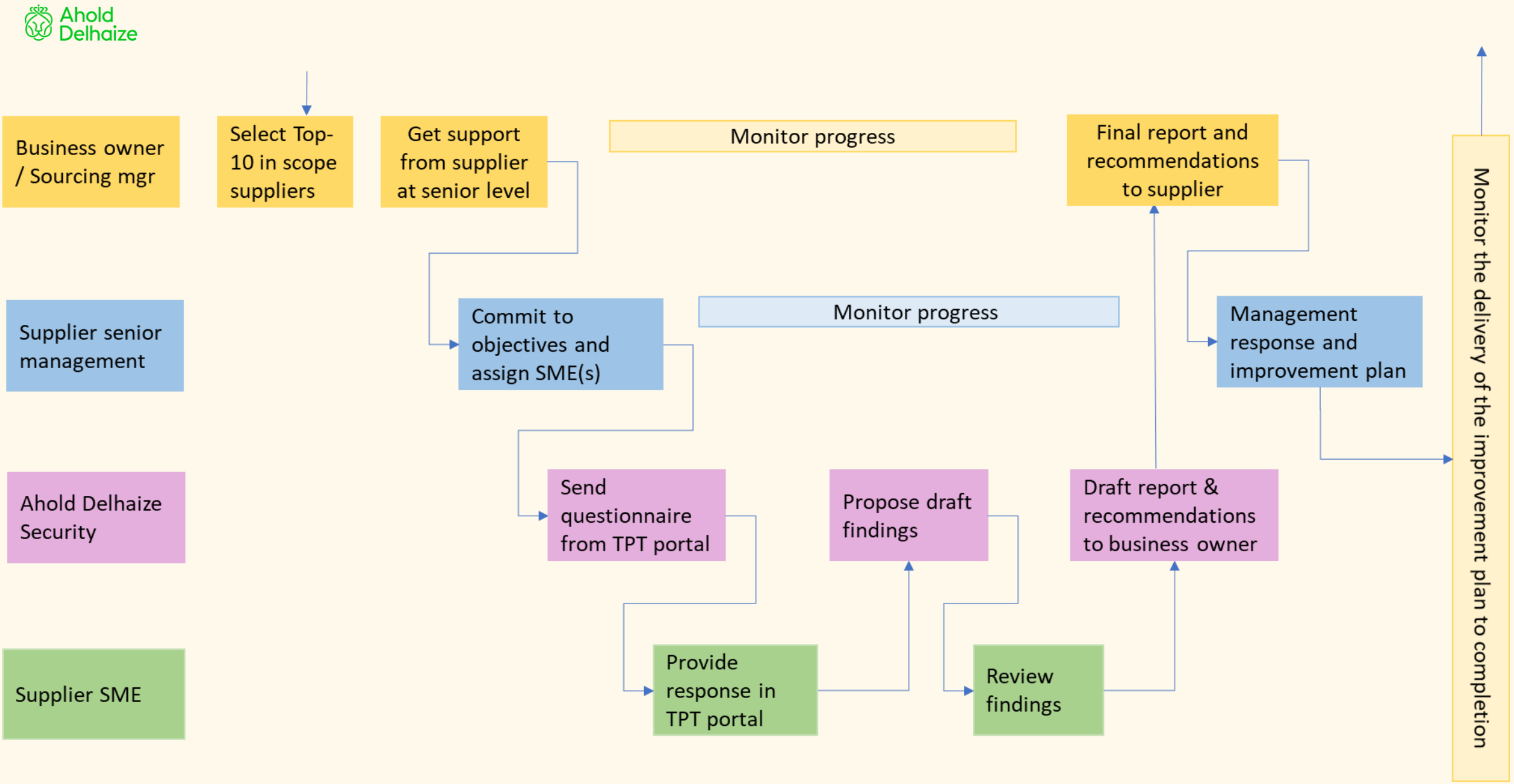
- **Periodieke bewaking van voortgang :**
  - Verbeterplan / management-reactie van supplier
  - AH SMEs kunnen op verzoek meedenken. Supplier is eindverantwoordelijk voor keuzes de ze maken
  - Bewaking van de voortgang van verbeteringen

# Samenwerking in de supply chain

- **Bouw Supplier Security Community:**
  - Regelmatige sessies om kennis te delen op het gebied van security processen, producten en implementaties
  - Delen van standpunten en leerpunten op het gebied van informatie beveiliging
  - Delen van Threat Intel.

# IT Security Addendum

- Contract addendum bestaande uit een aantal industrie standaard Security Controls.
- Gericht op de borging van beschikbaarheid van de IT van de supplier en de bescherming van de data van de supplier
- Het plan is om jaarlijkse reviews van de beheersmaatregelen uit te voeren, bij voorkeur door een onafhankelijke partij


Business owner / Sourcing mgr
Supplier senior management
Ahold Delhaize Security
Supplier SME
Select Top-10 in scope suppliers
Get support from supplier at senior level
Monitor progress
Commit to objectives and assign SME(s)
Monitor progress
Send questionnaire from TPT portal
Provide response in TPT portal
Propose draft findings
Review findings
Draft report & recommendations to business owner
Final report and recommendations to supplier
Management response and improvement plan
Monitor the delivery of the improvement plan to completion


15
PvIB
reconnect
in cyber security

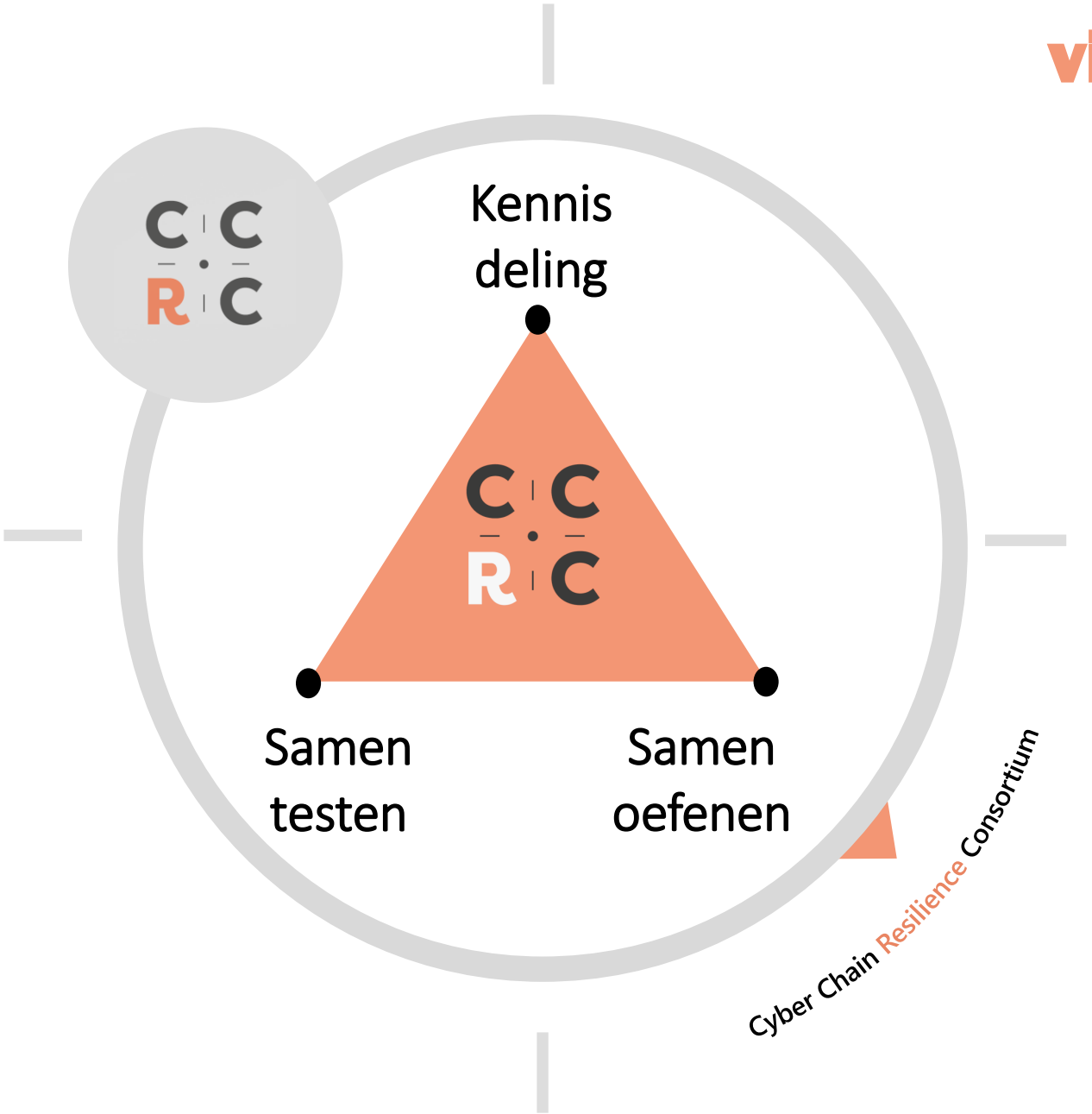
# IS DE LEVERANCIERS-KETEN CYBER WEERBAAR?

- We worden steeds meer afhankelijk van ketens door verregaande digitalisering
- End2end beveiliging wordt daarmee complexer
- Contractuele afspraken en audits is traditionele manier om grip te krijgen
- Ondanks goede afspraken gaat het regelmatig fout
- Met oefenen en testen verhogen we de weerbaarheid in de keten verder
- Samenwerking is hierbij cruciaal


The Cyber Chain Resilience Consortium is een platform waar publieke en private organisaties en hun leveranciers cross sectoraal samenwerken om zich te beschermen tegen moderne “Supply Chain Cyberaanvallen”.

Vergroot de cyberweerbaarheid van de leveranciersketen voor alle deelnemende bedrijven

# Onze visie




CCRC draag bij aan het verbeteren van de individuele cyberweerbaarheid van alle deelnemende bedrijven door het delen van kennis en het oefenen en testen van cyberaanvallen over de keten met een mindset van samenwerken

Cyber Chain
Resilience Consortium

Cyber Chain
Resilience Consortium

Philips, Eneco, Rabobank en Microsoft hebben zich al aangesloten.

Ook die extra stap zetten om de weerbaarheid te verhogen tegen cyber aanvallen via de keten?

Meldt je geheel vrijblijvend aan via de aanmeldknop op onze Linkedin pagina (QR code of link in de chat). We sturen dan aanvullende informatie en nemen contact met je op.

Of stuur een email naar:
Kelvin Rorive (kelvin.rorive@ccrc.nl)
Eric-Jan de Roode (ericjan.deroode@ccrc.nl)