TLP:GREEN

Red Teaming in de Zorg

COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

CERT

AGENDA

INTRODUCTIE

PRAKTIJK CASUS

Z-CERT

ZORRO

Q&A

Mitchell Sudmeijer

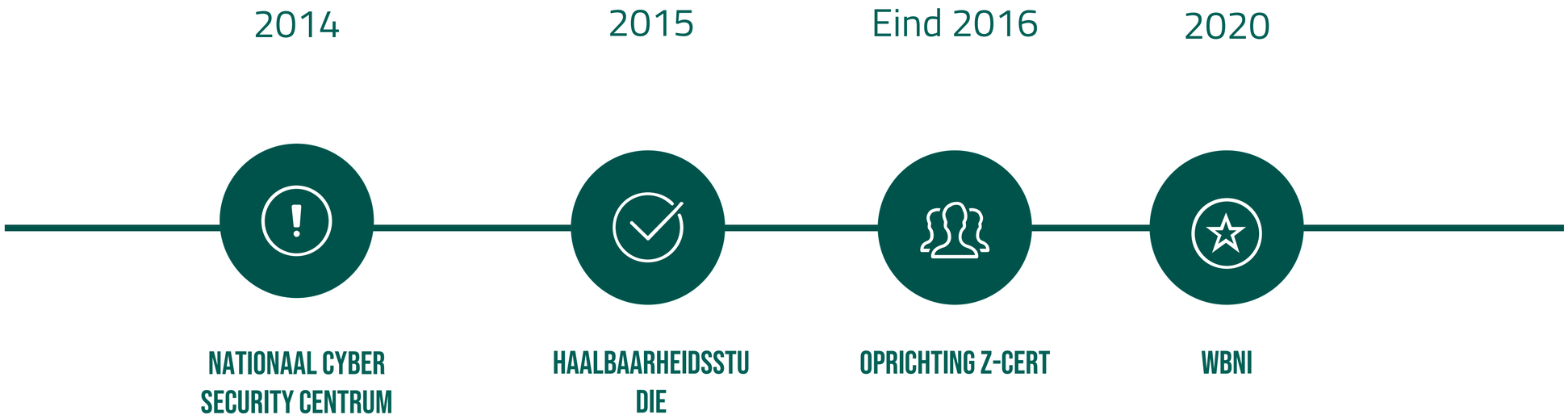
Information Security & Privacy Officer
MSC
SSCP, geslaagd voor CISM/CISSP/CCSP

Health Service Executive

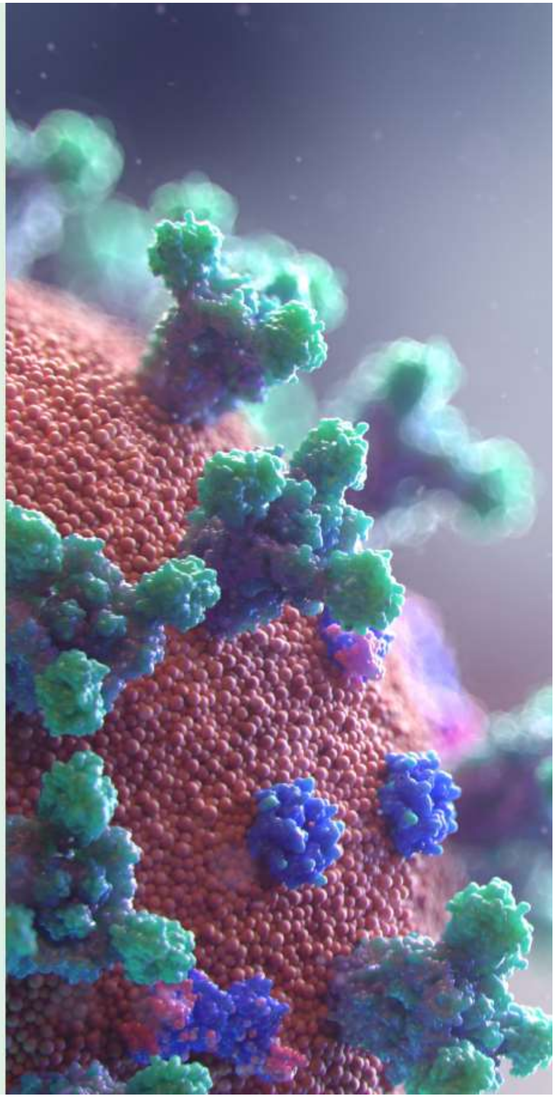
Feiten

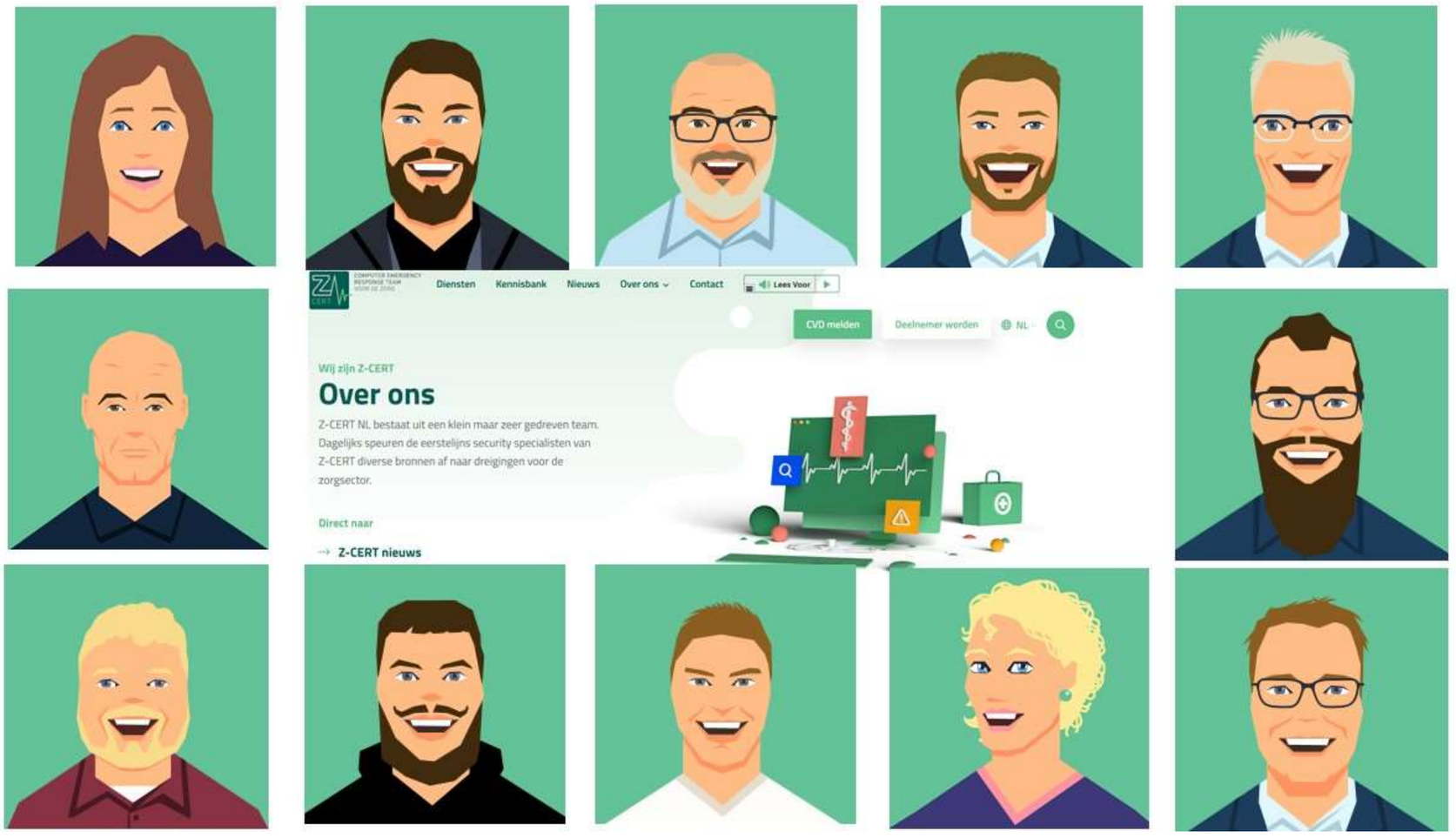
1. 80% versleuteld
2. 4 maanden herstelstijd
3. 700GB aan data gestolen
4. Velen claims
5. Enorme financiële schade
6. Veel leed

Tijdlijn


2014
2015
Eind 2016
2020
NATIONAAL CYBER SECURITY CENTRUM
HAALBAARHEIDSSTUDIE
OPRICHTING Z-CERT
WBNI

De missie van Z-CERT is het versterken van de digitale veiligheid van de zorgsector

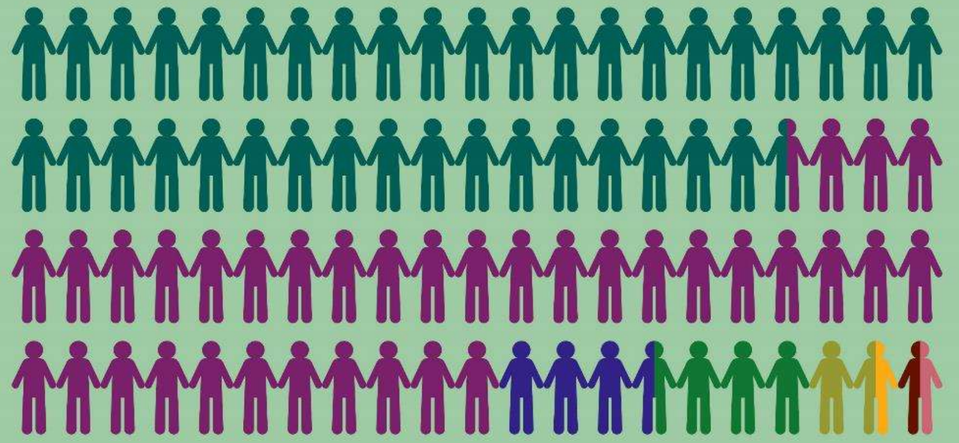



Diensten
Kennisbank
Nieuws
Over ons
Contact
Lees Voor
CVD melden
Deelnemer worden
NL
Wij zijn Z-CERT
Over ons
Z-CERT NL bestaat uit een klein maar zeer gedreven team. Dagelijks speuren de eerstelijns security specialisten van Z-CERT diverse bronnen af naar dreigingen voor de zorgsector.
Direct naar
Z-CERT nieuws

Deelnemers

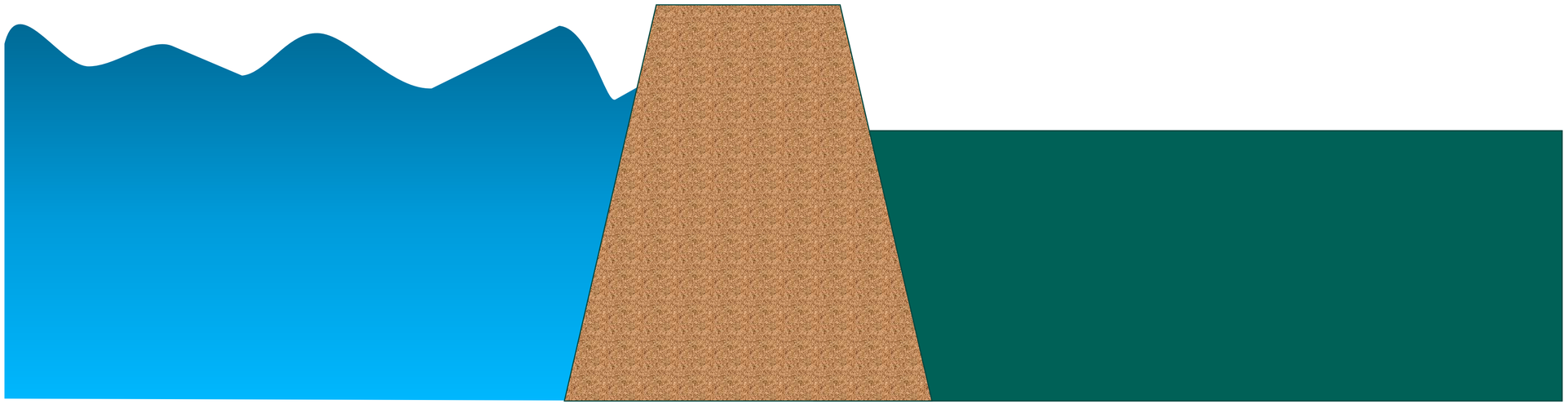
168* in totaal

- **NVZ** (77)
- **GGZ** (71)
- **NFU** (7)
- **ActiZ/VGN** (7)
- **Categoraal** (3)
- **Ambulance zorg** (1)
- **Jeugdzorg** (1)
- **Ziekenhuizen bijzondere gemeente** (1)



* Aantal deelnemers op 1 januari 2021

Cybersecurity



COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

Producten en Diensten

Stichting Z-CERT is hét expertisecentrum op het gebied van cybersecurity in de zorg. Z-CERT heeft specifieke kennis van medische hard- en software, ondersteunt zorgorganisaties bij een digitaal incident en vergroot de weerbaarheid van de sector op het gebied van cybersecurity.

Preventie

Kennisdeling

Z-CERT nodigt haar deelnemers uit om actief kennis te delen over hun aanpak van cybersecurity en waargenomen dreigingen.

Community

Z-CERT biedt een online platform aan waar deelnemers op een beveiligde omgeving onderling informatie kunnen uitwisselen. Z-CERT heeft hierin zowel een faciliterende als inhoudelijke rol. Tevens organiseert Z-CERT netwerkbijeenkomsten.

Informatieverzoeken

Deelnemers kunnen een niet-urgente security vraag via e-mail of een beveiligd chatkanaal voorleggen aan de specialisten van Z-CERT.

Publicaties

Z-CERT deelt verdiepende kennis over cybersecurity onderwerpen zoals ransomware via whitepapers en factsheets.

Preventie

Informatieberichten en alertering

Z-CERT ontvangt informatie van het Nationaal Cyber Security Centrum, andere (inter)nationale CERTS en partners. Z-CERT vertaalt deze informatie naar de volgende producten.

(Medische) Advisories

± 50 per maand

Advisories met handelingsadvies over ontdekte kwetsbaarheden in (medische) hard- / software.

Infoberichten

± 7 per maand

Informatie over lopende security incidenten met sector brede impact.

Operational alerts

± 1 per maand

Informatie over actuele en urgente dreigingen waarbij Z-CERT de ontvanger oproept direct te handelen (bijv. patchen).

End-of-week

Een wekelijks overzicht van alle verzonden advisories, (relevante) mediaberichten en links naar websites met achtergrondinformatie.

End-of-month

Een maandelijks overzicht van relevante ontwikkelingen en actualiteiten met een duiding door de experts van Z-CERT.

Detectie

Monitoring IP-adressen en domeinnamen

Z-CERT controleert elke werkdag of IP-adressen en domeinnamen van deelnemers op blacklists voorkomen. Daarnaast ontvangt Z-CERT regelmatig lijsten met kwetsbare systemen van zorginstellingen, zoekt proactief naar kwetsbare systemen of stelt deze lijsten zelf samen.

ZorgDetectieNetwerk (ZDN)

Deelnemers kunnen kiezen voor een aansluiting op het ZDN. Het ZDN deelt realtime 'indicators of compromise' met deelnemers. Deze informatie vormt een collectief geheugen voor digitale dreigingen met als doel een weerbare zorgsector.

Response

Afhandeling en coördinatie incidenten

Wanneer een deelnemer te maken heeft met een IT-beveiligingsincident, adviseert Z-CERT bij de aanpak en het oplossen van het incident. Tevens kan Z-CERT ondersteuning bieden bij forensisch onderzoek.

Coordinated Vulnerability Disclosure

Kwetsbaarheden in websites van deelnemers en in (medische) apparatuur of programmatuur, die door derden zijn ontdekt, kunnen bij Z-CERT worden gemeld.

Preventie

Z-CERT Stationsplein 121, 3818 LE Amersfoort www.z-cert.nl

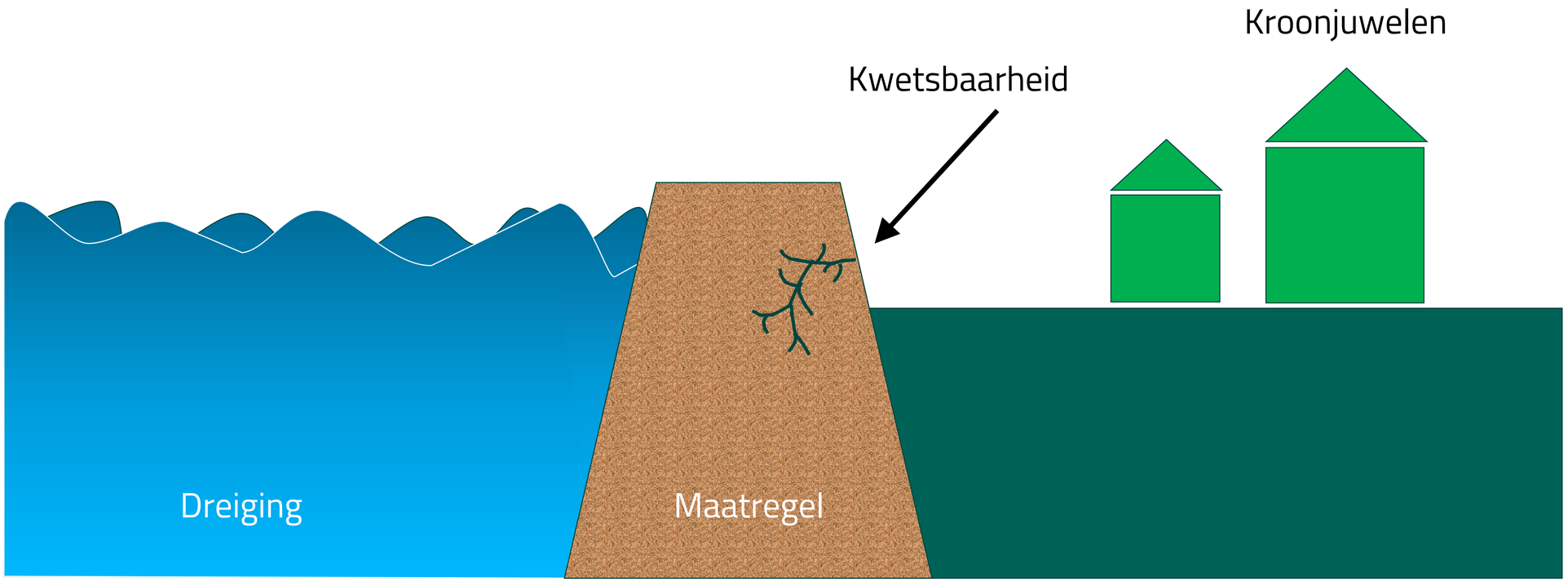
Mijn naam is

Marcel Tegelaar

Senior security consultant met ervaring op zowel organisatorisch als technisch vlak. Informatica gestudeerd aan de TU Delft. Vervolgens als programmamanager werkzaam geweest en diverse security rollen vervuld voor meerdere organisaties.

Binnen Z-CERT betrokken bij Red Teaming in de zorg (ZORRO), een haalbaarheidsstudie SOC/SIEM voor de zorgsector en de bijdrage aan de ONE conference voor de Europese Health ISAC.

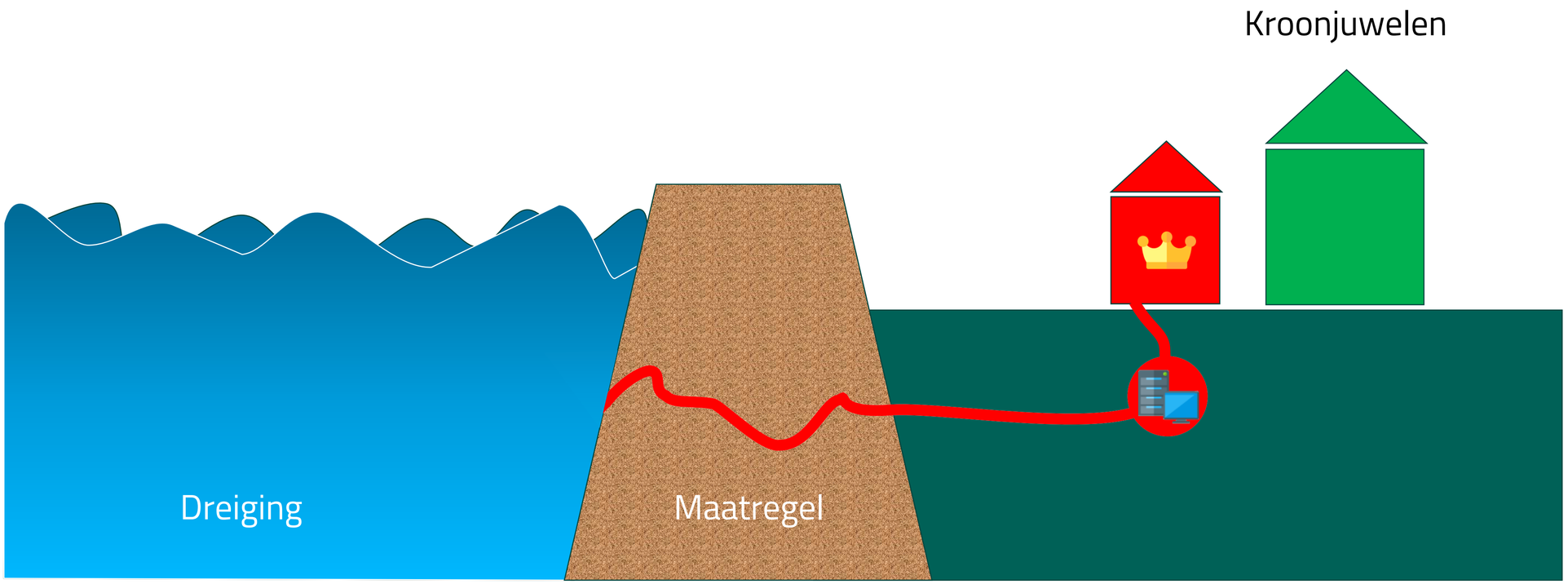
Preventieve maatregelen & Kwetsbaarheden



“

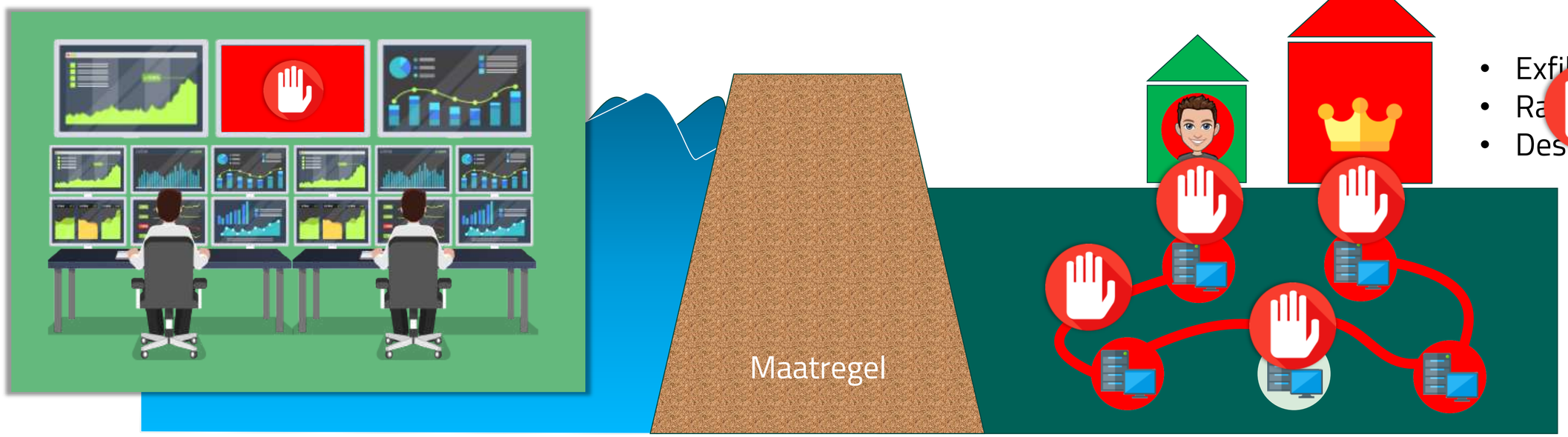
”

Penetratietesten: Technische kwetsbaarheden



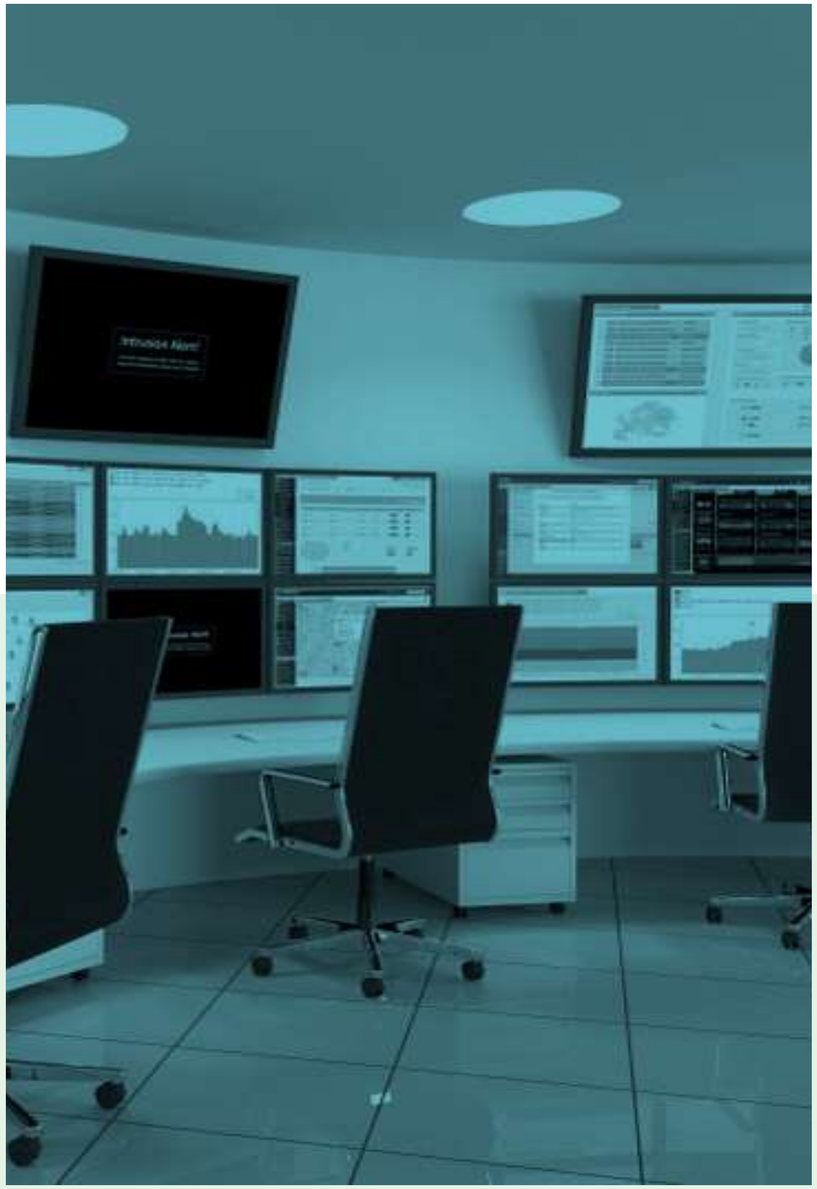
Red Teaming: Simulatie van een realistische aanval

(Voorbeeld)
Spearphishing e-mail



Kenmerken Red Teaming

- Realistische aanvallen
- Op basis van actuele dreigingen
- “Onder de radar”
- Inzicht in detectie & response



De ZORRO aanpak

Achtergrond

- **ZORRO** = **Zo**rg **R**edteaming **R**esilience **O**efeningen

- Geïnspireerd door TIBER
    - Threat Intelligence Based Ethical Red-teaming
    - Succesvol in financiële sector, verzekeringen, energie
    - Binnenkort verplicht voor de Nederlandse overheid
    - Europese adoptie

ZORRO is specifiek voor de zorgsector

- Veiligheid verbeteren van individuele deelnemers en de zorgsector als geheel

- ZORRO is een aanpak op maat voor de zorgsector
  - Kortere doorlooptijd, lagere kosten
  - Zorgspecifieke dreigingen, incidenten, actoren, scenario's en risico's
  - Samenwerking binnen de zorgsector

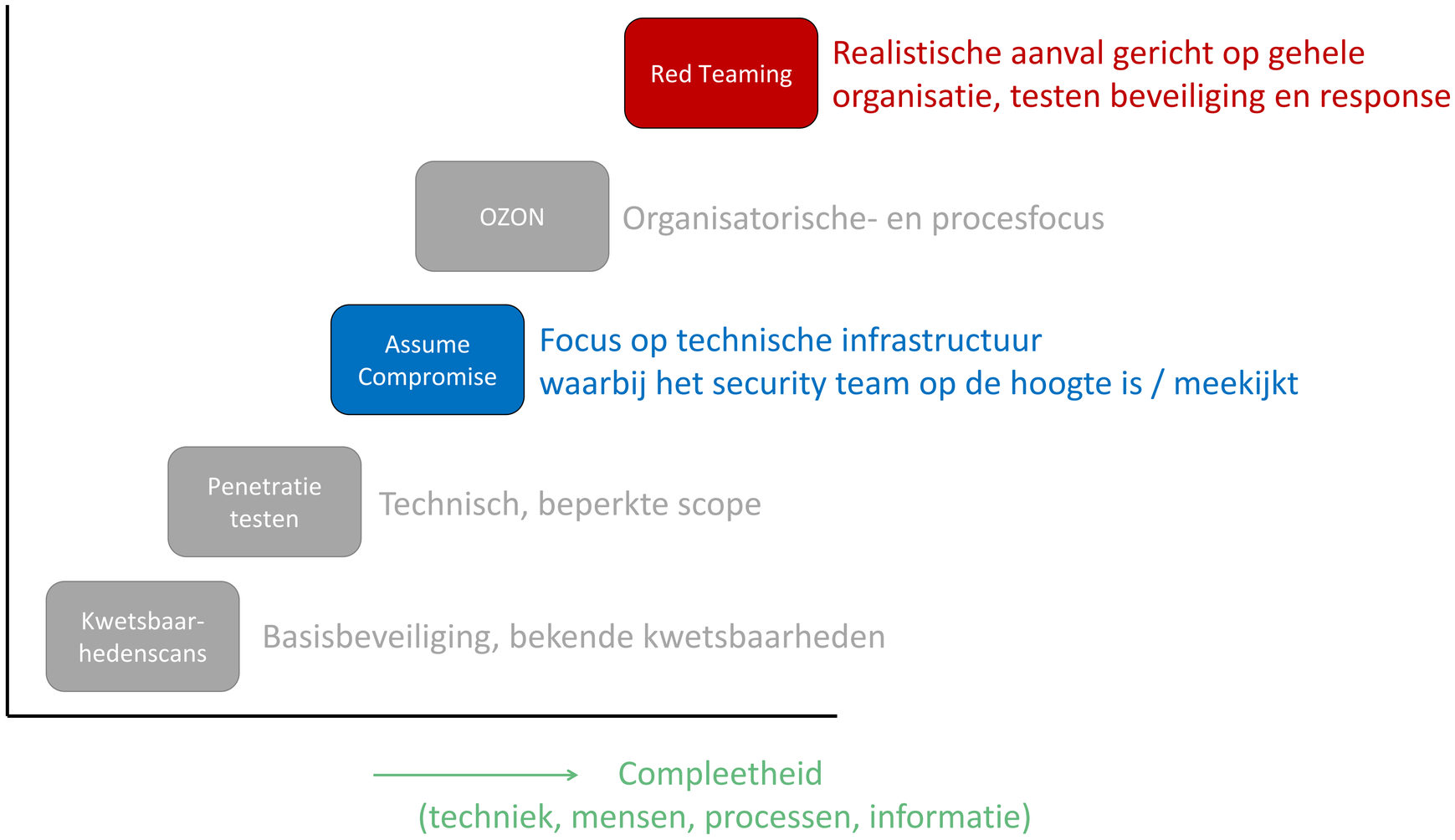
- Threat intelligence en testscenario's
  - Op basis van sectoriale kennis
  - (Niet-openbare) informatie van deelnemers

Wat levert het op?

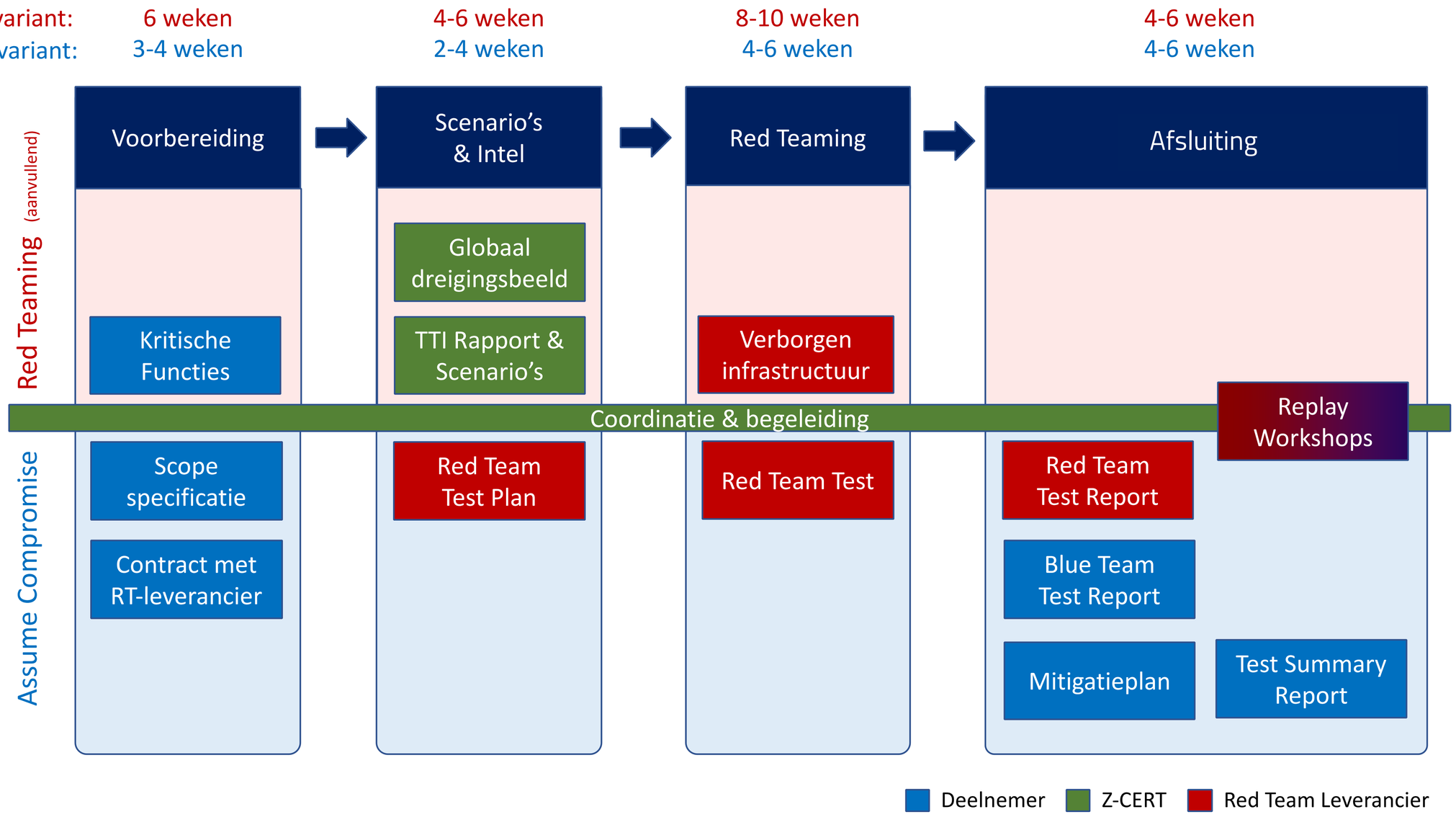
- Bewustwording en aandacht op bestuursniveau
  - Realistische aanval
  - Kroonjuwelen worden geraakt

- Verbeterkansen in processen en techniek
  - Tactieken, Technieken en Procedures (TTP)
  - Detectie en response

Positionering ZORRO



ZORRO aanpak kent 2 varianten



Red Teaming fase

- Gebaseerd op het scenario:
  - IN - 1-2 weken
  - THROUGH - 3-4 weken
  - OUT - 1-2 weken
  - Leg-ups

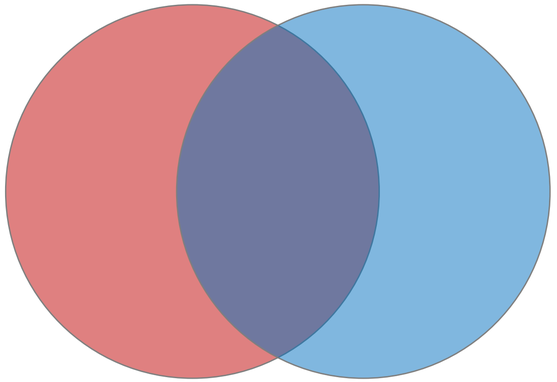
- Intensieve communicatie / afstemming
  - Red Team en White Team (continu)
  - Red Team lead, White Team lead, ZCT (wekelijks)

Purple Teaming

- Leren van de aanval en identificeren verbeterkansen

    - Naspelen aanval en detectie (1-2 dagen)
    - Vergelijken informatie van Blue Team en Red Team
    - Bespreken alternatieve technische aanvallen

    - Verbeteren detectie en response
    - Verbeteren escalatie- en communicatieprocessen



Rol van Z-CERT

- Expertisecentrum voor cybersecurity in de zorg
    - ZORRO Cyber Team (ZCT)

- Z-CERT levert voor iedere ZORRO test:
    - Globaal dreigingsbeeld
    - Targeted Threat Intel rapport
    - Aanvalsscenario
    - Begeleiding methodiek
    - Faciliteren kennisdelen deelnemers

Rol van het White Team

- Risicomanagement
    - Kritische functies en scope
    - Goedkeuring op testplan en activiteiten
    - Inventariseren en wegen risico’s

- Voorkomt ongewenste escalaties
    - Voelsprieten in zorgproces, SOC, etc.
    - (Externe) escalaties tegenhouden

- Heeft een virtuele stopknop

Rol van het Red Team

- Opstellen testplan
    - Scenario uitwerken naar concreet aanvalsplan
    - Leg-ups definiëren
- Uitvoeren gesimuleerde aanval
    - Communicatie, communicatie, communicatie
- Purple teaming

Rol van het Blue Team

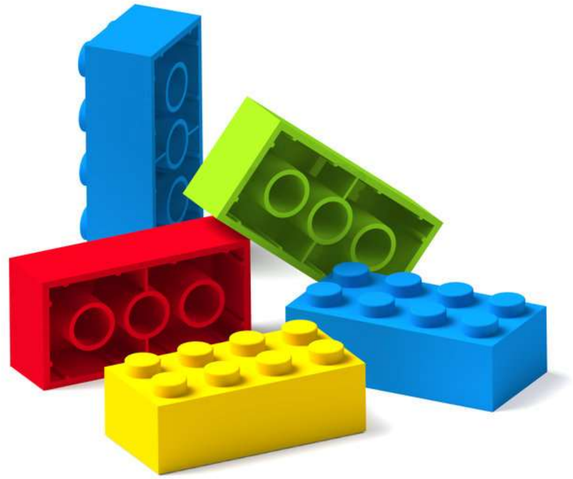
- Business as usual
    - Detectie & response

- Vooraf niet geïnformeerd
    - Realistische aanval

- Verbeterkansen
    - Deelname Purple Teaming
    - Verbeteren detectie & response

ZORRO Toolkit

- ZORRO aanpak
- Curated lijst van Red Team leveranciers
- Templates
  - Scope specificatie
  - Targeted Threat Intel
  - Generieke activiteitenplanning
  - Bijlage voor offerte-aanvraag

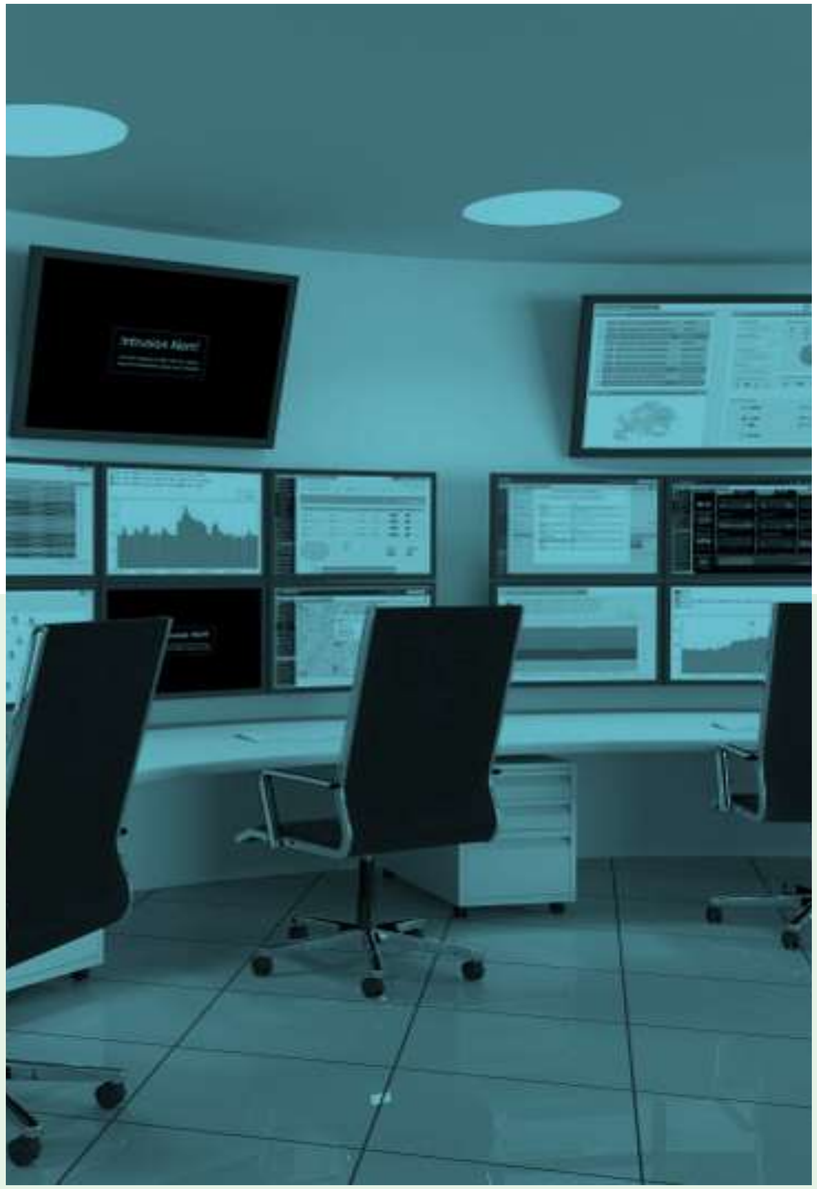


Kennis delen binnen ZORRO community

- Alle deelnemers laten profiteren

- Delen van uitgevoerde acties en resultaten
    - De deelnemer bepaalt mate waarin informatie wordt gedeeld

- Z-CERT adviseert op basis van eerdere resultaten
- Ervaringen met Red Teaming-leveranciers



Start in 2021, nu verder

ZORRO voor Antoni van Leeuwenhoek ziekenhuis

- Codenaam Gallus
- Joost Boele, CISO van het AVL:

“Zo krijg je inzichten die je met losse testen nooit zou kunnen krijgen. Bovendien heb je als instelling een sluitend verhaal, gebaseerd op een realistische dreiging, om het informatiebeveiligingsbewustzijn van zorgverleners, onderzoekers, technici en managers mee te vergroten.”

Bredere uitrol ZORRO-testen is gestart in 2022

- Deelnemer met codenaam Asklepios
  - (Oudgrieks: Ασκληπιός, Asklepios; Latijn: Aesculapius; Nederlands Asclepius) is in de Griekse mythologie de god van geneeskunde en genezing.
- Meerdere testen

Meer weten?

Stichting Z-CERT

www.z-cert.nl