TLP:GREEN

Starten met Cyber trainen en oefenen

COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

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

Introductie

Auke Nicolaï

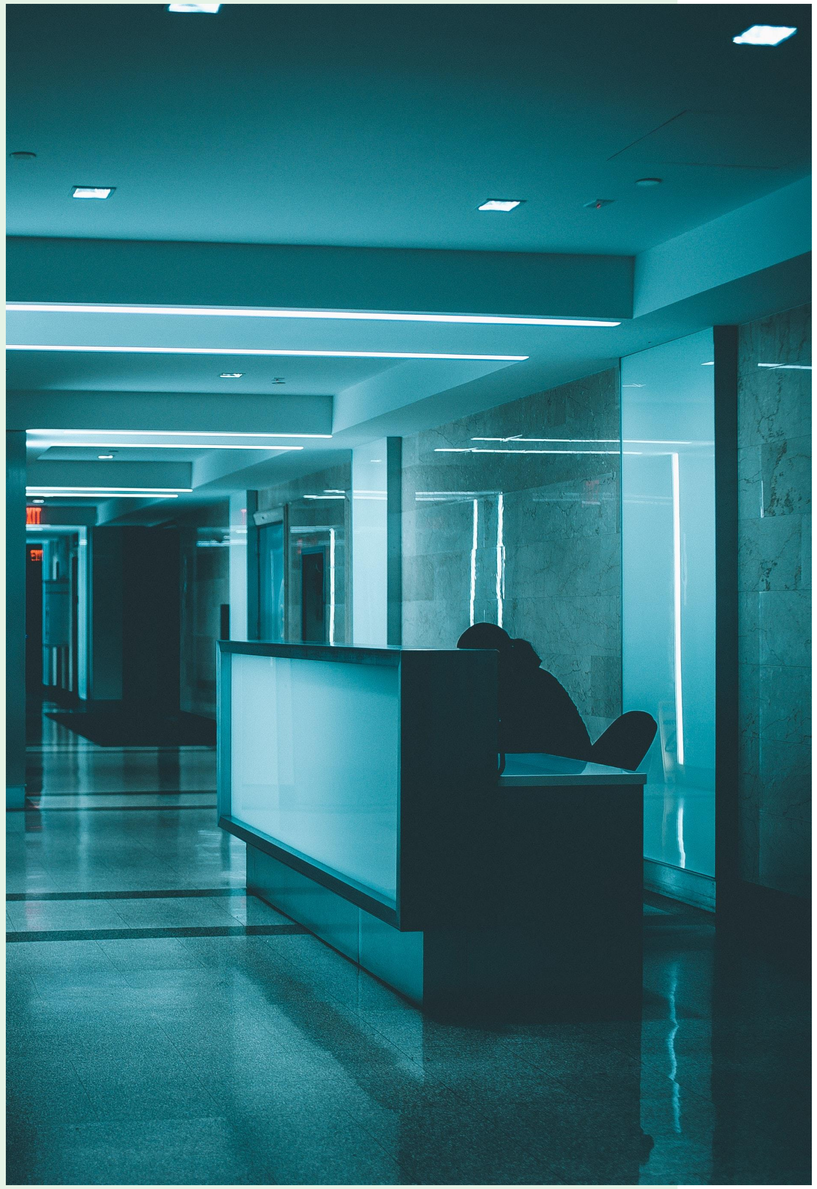
Business Consultant

- ziekenhuizen
- acute zorg
- eerstelijns zorg

Jeroen Brouwer

Business Consultant

- GGD-GHOR
- thema oefenen



Oefenen in de praktijk

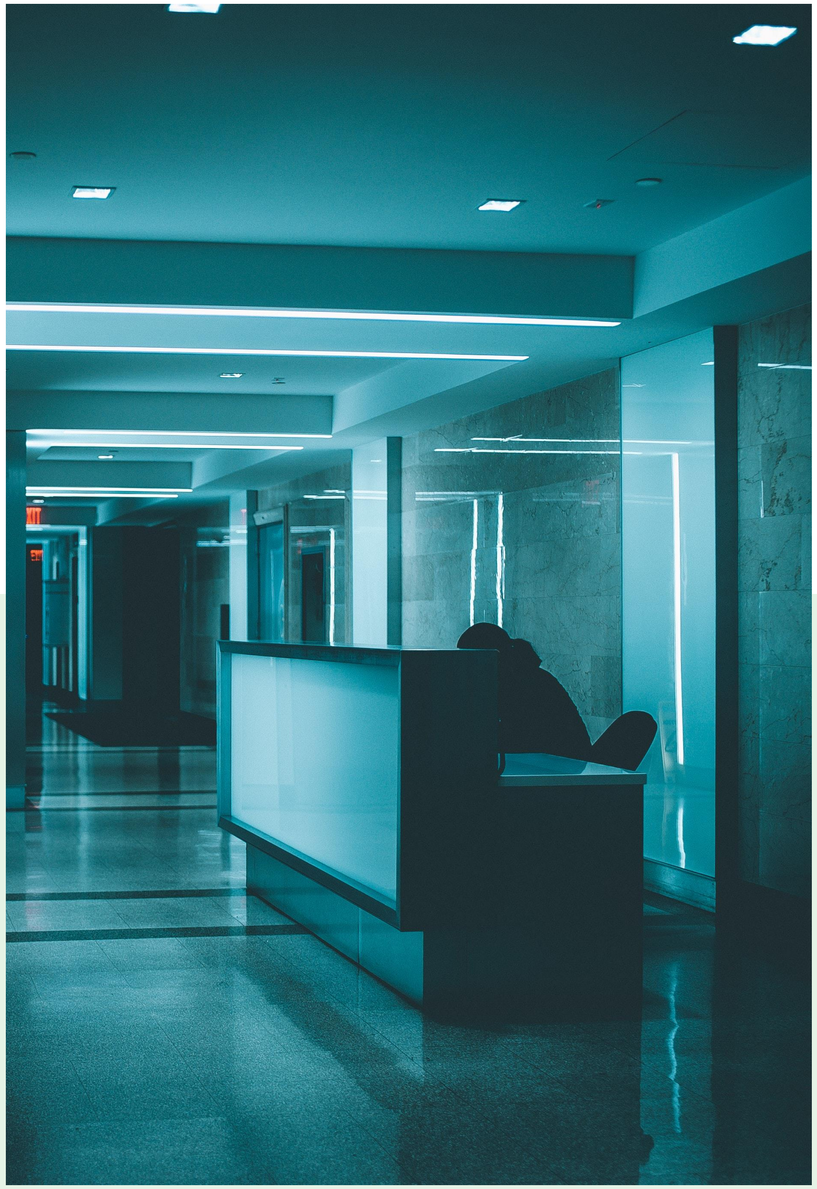
Rondje langs de velden…

- wie heeft al eens geoefend?
- wat voor soort oefening?
- wat was de opbrengst?
- wat is er daarna in de organisatie merkbaar veranderd?

Waarom oefenen?

Stel: oefeninterland spelen met deze opstelling

- Gedachten?



Starten met cyber trainen/oefenen

Waar te beginnen en hoe aan te pakken?

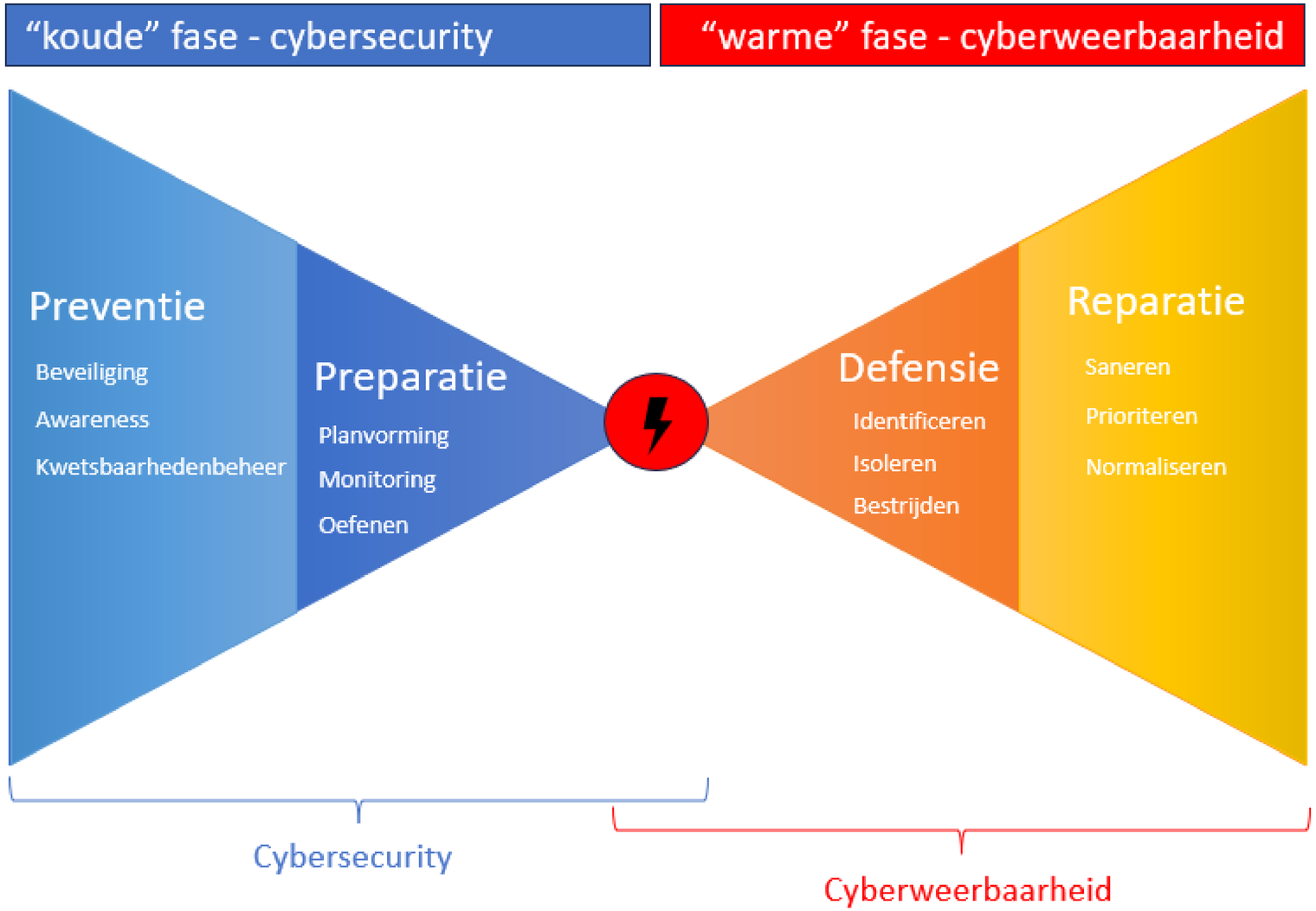
In dit document introduceren we het onderwerp en delen we onze belangrijkste tips.

Waarom oefenen zo belangrijk is

We geven een aantal redenen waarom oefenen zo belangrijk is voor elke organisatie:

- Kennis leidt niet altijd tot gedrag. Er zijn allerlei redenen waarom mensen niet in beweging komen, ook al weten ze wel wat ze zouden willen doen. In een oefensetting is er ruimte om gedrag te signaleren en bij te sturen.
- Tijdens incidenten zijn andere vaardigheden nodig dan in een normale situatie. Deze vaardigheden maken lang niet altijd deel uit van een functieprofiel en bijbehorende opleidingen.
- Durven doen. In een crisissituatie ligt veel druk op handelen en ligt de crisisorganisatie onder een vergrootglas. Dat kan leiden tot een 'freeze' bij individuen of er ontstaat besluiteloosheid in de teamdynamiek.
- En wellicht de belangrijkste: tijdens een crisis lijk je in een andere organisatie te zijn beland. Er gaan zoveel zaken anders dat je niet kunt terugvallen op bekend terrein.

Cybersecurity is nog geen cyberweerbaarheid



Wat is wat

Hieronder een beknopte duiding van termen, zonder formele definities te willen geven:

- Opleiden is benodigde kennis verwerven
- Trainen is groeien in een bepaalde rol door ervaring op te bouwen
- Oefenen is het toepassen van de rol die je tijdens een calamiteit hebt in een oefensituatie
- Testen is bepalen of beveiligingsmaatregelen naar verwachting werken. Dat laten we in dit document buiten beschouwing.

Kaders uit de NEN7510 en de CyberBeveiligingsWet (NIS2)

De NEN7510 :

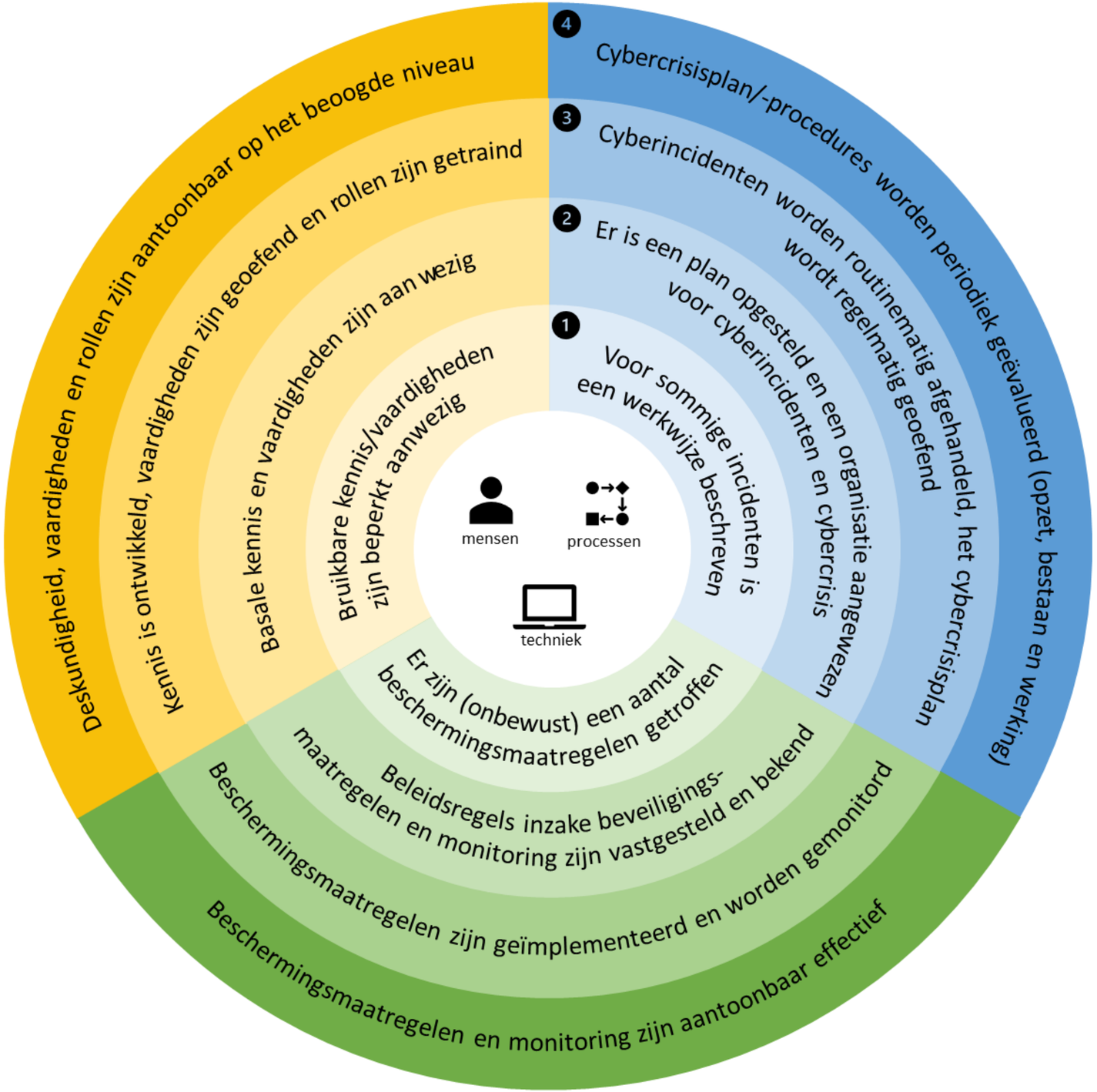
- ontwikkelen van competenties door opleiding, training en ervaring (7.2.2)
- borgen van bewustzijn m.b.t. beleid en procedures (7.3)
- programmatisch in de praktijk toetsen van continuïteitsplannen (17.1.1)
- verwerven van routine en kennis over – en vaststellen van de werking van – continuïteitsmaatregelen en procedures (17.1.3)

In de CyberBeveiligingsWet (NIS2) worden 'bedrijfscontinuïteit', 'noodvoorzieningenplannen' en 'crisisbeheer' genoemd als *minimaal* onderdeel van de vereiste maatregelen.

Tips om te beginnen, om te groeien en om op niveau te blijven

Begin eenvoudig. Een heel belangrijk principe voor alle interventies (opleidingen, trainingen en oefeningen) is dat ze moeten aansluiten bij de organisatie. Als interventies onvoldoende passen bij de organisatie (op dat moment) kom je niet verder, maar verminderd juist het draagvlak. Als je aan het begin staat van OTO, zorg dan ook dat jouw interventies geen voorkennis vereisen.

Tips om te beginnen



Weet waar je staat. Neem de tijd om te kijken waar je staat en wees daar realistisch in. Wellicht is het nodig om verschillende delen van de organisatie ook verschillend in te schalen

Tips om te beginnen

Lage complexiteit, hoog risico. Pak eerst de hoge risico's met een lage complexiteit aan. Daardoor maak je meteen impact, zonder te veel hooi op je vork te nemen. Dat versterkt het draagvlak in de organisatie.

Generiek boven maatwerk. Gebruik in eerste instantie vooral generieke en bewezen templates en voorbeelden. Er is veel te vinden op internet en bij de collega's in de zorg. Dat beperkt de initiële investering en in de praktijk blijkt dat hiermee een goede start kan worden gemaakt. Bij een hogere volwassenheid gaat maatwerk een steeds grotere rol spelen.

Creëer draagvlak. Als je weet hoe je wilt starten, wordt het creëren van draagvlak van belang. Wees helder over verwachtingen en neem alle relevante rollen mee.

Continu verbeteren (PDCA). Geen nieuws, maar ook hier geldt dat een beheerst en gepland proces helpt in het groeien in volwassenheid. Niet alleen omdat je weet wat je te doen staat, maar ook omdat het naar de omgeving toe duidelijkheid geeft en de juiste verwachtingen schept.

Kies het juiste doelniveau. Wees hierin ambitieus, maar altijd haalbaar. Voor deze tip is het cruciaal om de eigen organisatie goed te kennen. Soms heeft een organisatie het nodig om ambitieuzer te zijn om het gebeid van security. Soms om realistischer te zijn. Maak hier je keuzes in overleg met bestuur / senior management. Zij kunnen dit enerzijds goed inschatten en anderzijds is hun steun onmisbaar.

Start met parallel borgen. Wacht niet met het borgen van oefenen in rolbeschrijvingen, processen en werkinstructies, maar begin daar juist mee. Natuurlijk moet je hier ook mee afsluiten, maar door hiermee te beginnen creëer je al zoveel formeel draagvlak en kun je hindernissen wegnemen. Doe het wel parallel, want hier kan de bureaucratie ook vertragend werken.

Tips om te groeien

Rol	Taak	Competenties
CrisisLeider 	Leiding & Coördinatie	Accuraat, Stressbestendig, Samenwerken, Analyseren, Plannen, Organiseren en coördineren, Politiek-bestuurlijk inzicht, Daadkracht
InformatieManager 	Informatiemanagement	Accuraat, Stressbestendig, Samenwerken, Analyseren, Organiseren en coördineren
Communicatie Manager 	Crisiscommunicaties	Accuraat, Stressbestendig, Samenwerken, Politiek-bestuurlijk inzicht, Communiceren, Inleven, Maatschappelijk georiënteerd
Materiedeskundige 	(Strategische) Advisering	Accuraat, Stressbestendig, Samenwerken, Analyseren, Communiceren

Tips om te groeien

Vergeet je omgeving niet. Security is geen eiland en je organisatie ook niet. Neem bij het oefenen en het borgen van verbeteringen ook de minder voor de hand liggende partijen mee. Denk aan architecten en leveranciers.

Werk risico gestuurd. Probeer risico's te benaderen als kansen voor cybercriminelen. Betrek (interne) experts en vertrouw op hun oordeel. Geef het grootste risico het eerst aandacht.

Tips om op niveau te blijven

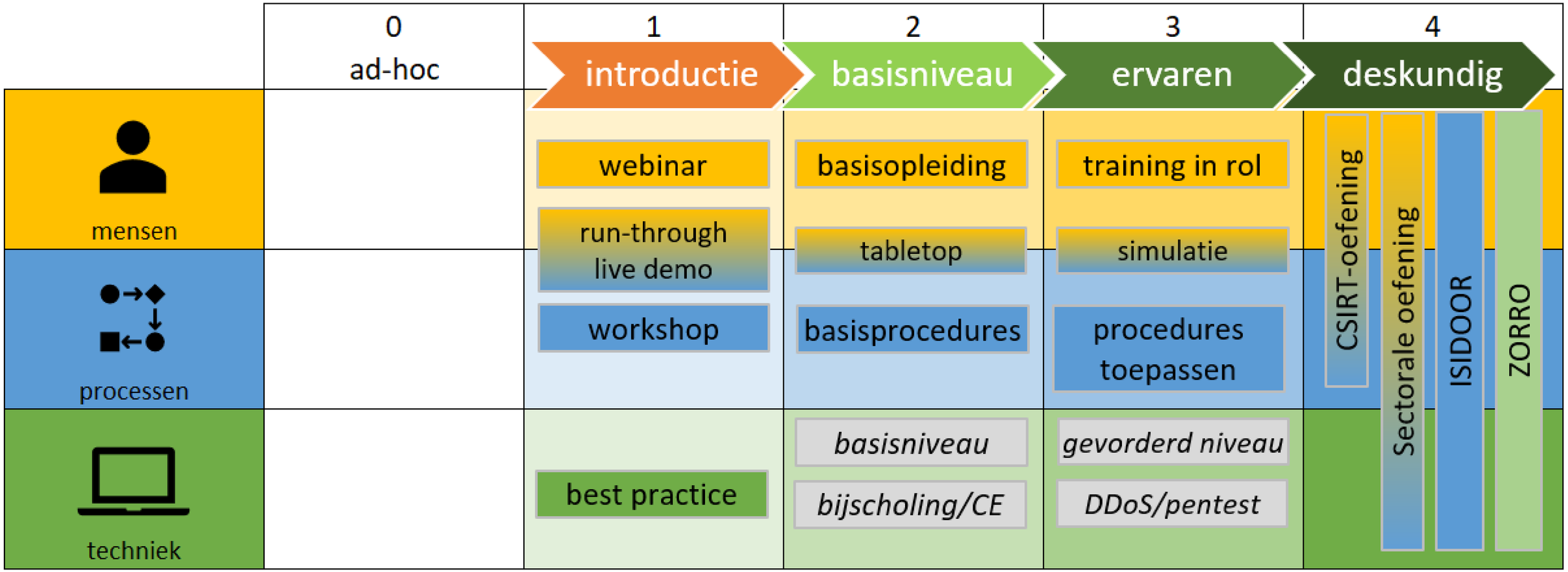
Blijf in het ritme om te winnen in kwaliteit en efficiëntie. Een valkuil van volwassenheidsniveaus is denken dat je klaar bent. Je bent nooit klaar. Zorg dat de organisatie werkt in een oefenritme. Vastgelegd in processen en agenda's. Juist als oefenen niet meer gericht is op een ander niveau, dan kan het zich richten op kwaliteit en efficiëntie. De kracht van herhaling.

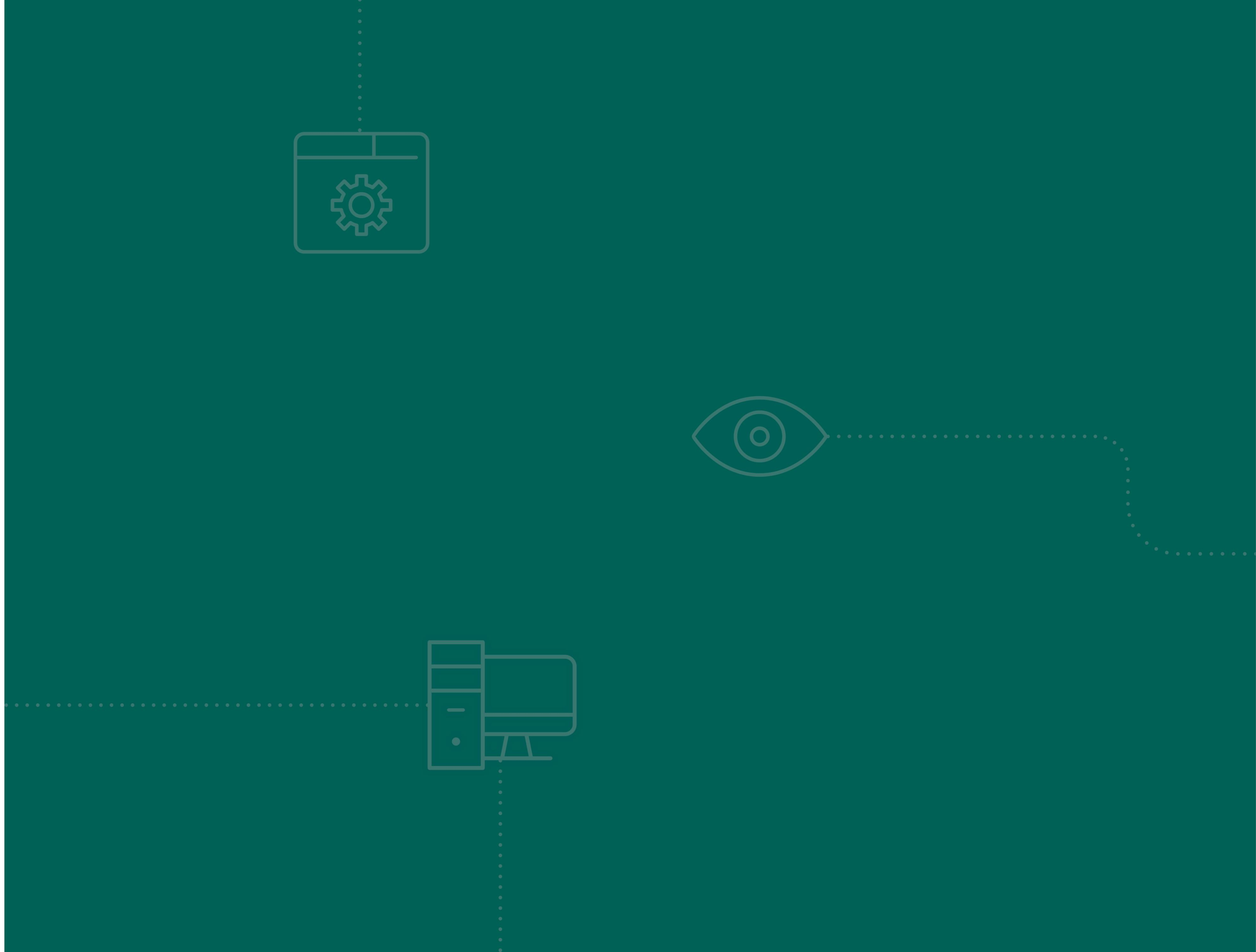
Beweeg mee met je architectuur en je leveranciers. Een volwassenheidsniveau borgen betekend dat wijzigingen in de architectuur (IT en anderszins) ook verwerkt worden in het oefenen. Zowel de interne omgeving als die van leveranciers. Want hoe rampzalig kan een incident uitpakken, als je oefent op een achterhaalde situatie?

Vragen/opmerkingen?

- helpt dit jouw organisatie?
- wat mis je nog/wat kan anders?
-feedback welkom!

Vervolg (cliffhanger voor sessie 2)





Stichting Z-CERT

www.z-cert.nl