



OT & CYBERSECURITY CONFERENTIE



22 April 2026 • Amersfoort

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

OT Coalitie



Onze havens zijn cruciaal voor Europa



32% van de containers



50% van de totale overslag



Host nation Support



Voedsel en medicijnen



Nr. 1 in Europa

OT & CYBERSECURITY CONFERENTIE



ProRail



Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

OT Coalitie



Verandering in dreigingslandschap



Ongericht

Ongericht

- Inbrekers
- Fraudende medewerker
- Scriptkiddies



Doelgericht

Doelgericht

- Activisten
- Beroepskrimen (uithalers)
- Cybercriminelen



Langdurig & doelgericht

Langdurig & doelgericht

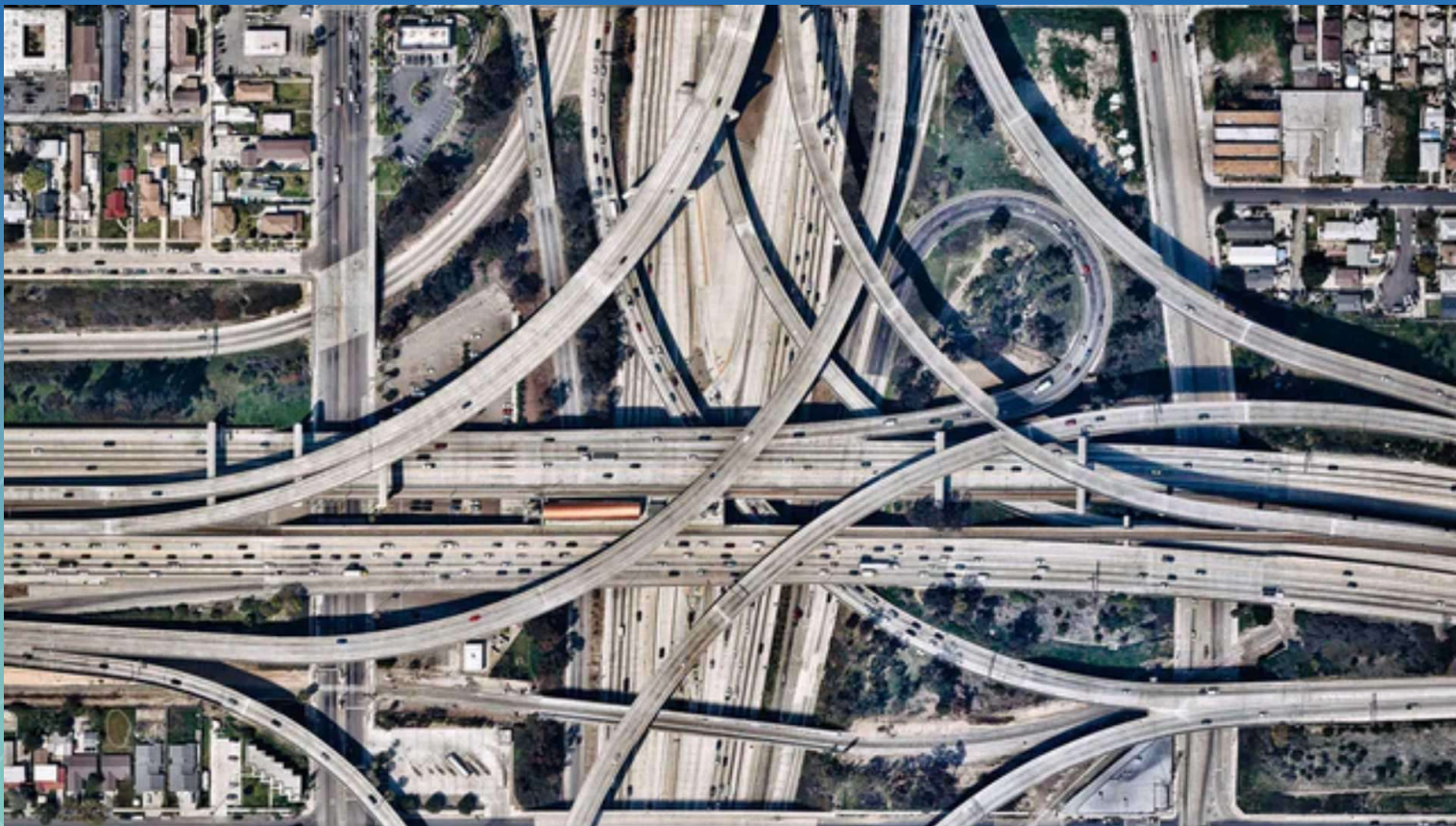
- Terrorisme
- Statelijk actoren

Laag

Intentie en capability die voorhanden zijn voor de actor en acties

Hoog

OT & CYBERSECURITY CONFERENTIE



Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

OT Coalitie



De CYRA-methode

- **Inzicht**
Het self-assessment geeft waardevolle inzichten over de status van de digitale weerbaarheid van de organisatie
- **Groeiperspectief**
CYRA biedt een duidelijk stappenplan (groeipad) om de cybersecurity te verbeteren (controls & maturity)
- **Vertrouwen**
Mogelijkheid tot onafhankelijke beoordeling (certificeren)



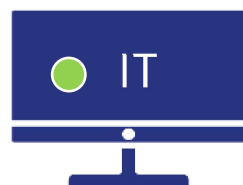
De CYRA-methode

- Gebaseerd op risicoanalyse: door eigen organisatie en/of door opdrachtgever i.r.t. leveranciersmanagement
- Leverancier investeert één keer en kan zelfverklaring en certificaat hergebruiken
- Draagt bij aan invulling NIS2 richtlijn (zorgplicht)
- Gericht op supply chain

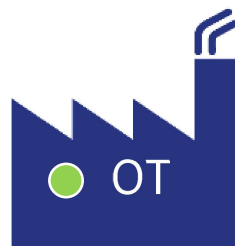


De CYRA-modules

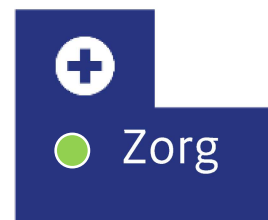
CYRA | Cyber Rating



ISO 27001 /
ISO 27701



IEC 62443



NEN 7510



Waarom gebaseerd op IEC 62443?

- Gebaseerd op IEC 62443-2-1 (beheerprocessen) & IEC 62443-3-3 (technische maatregelen)
- Internationaal erkende OT-cybersecuritynorm
- Richt zich op processen en techniek bij asset owners
- Sluit aan bij best practices en regelgeving



30%

Entry level

Level 1
Ad Hoc



Level 2
Best effort



Level 3
Defined



60%

Basic level

Level 1
Ad Hoc



Level 2
Best effort



Level 3
Defined



80%

Inter-
mediate
level

Level 1
Ad Hoc



Level 2
Best effort



Level 3
Defined



100%

Advanced level

Level 1
Ad Hoc

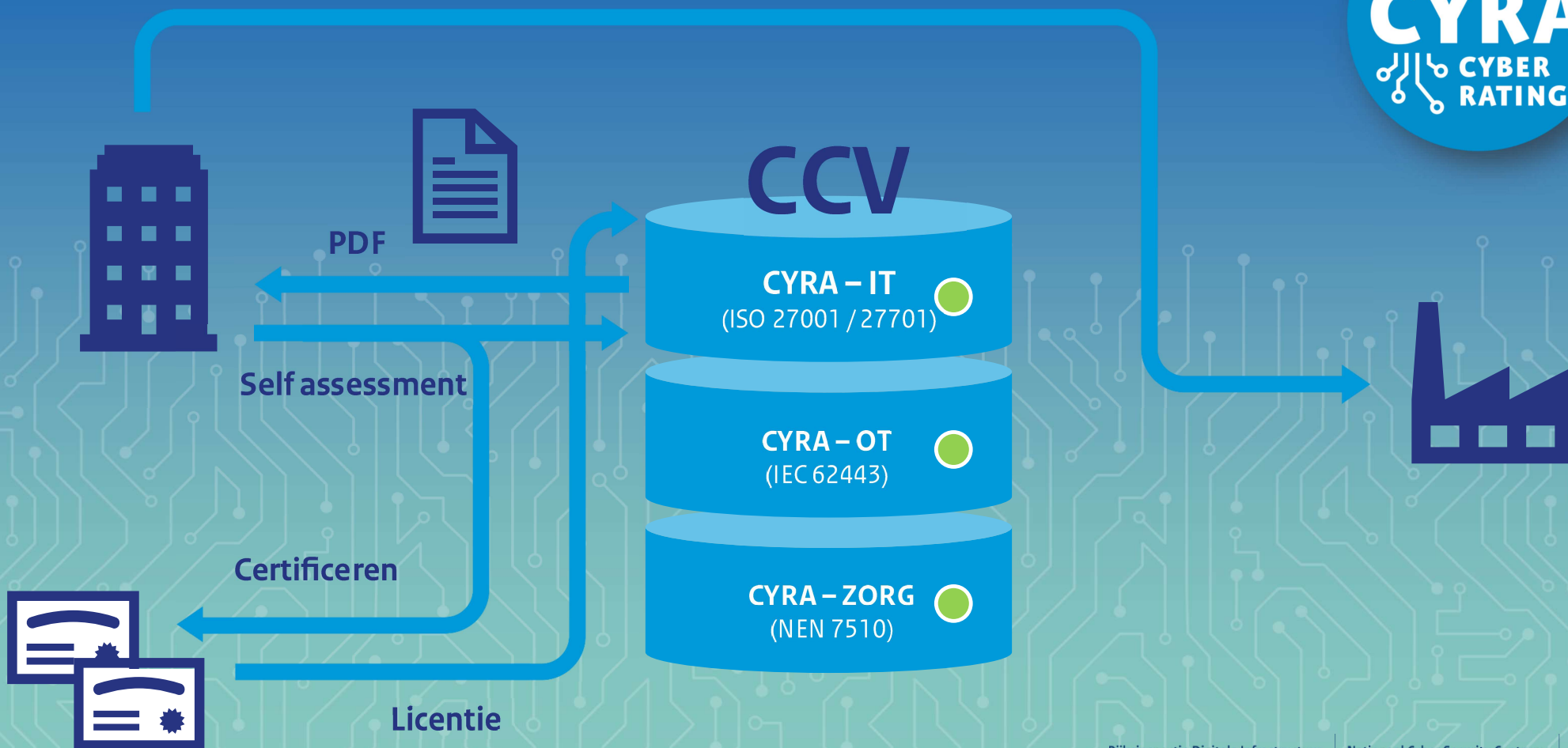


Level 2
Best effort



Level 3
Defined







Leveranciersmanagement OT

- Objecten & systemen zijn *'built to forget'*
- Langlopende contracten
- De spoeling is dun
- Maatwerk oplossingen
- Versnipperd eigenaarschap & verantwoordelijkheden

In OT hangt alles aan elkaar, maar niemand bezit het geheel



Walk the talk!

Eisen stellen is makkelijk !!



Maar ga je er ook op toezien ??

Zorg dat het geen papieren tijger wordt

Wij willen een volwassen partij !!



Ben je bereid in gesprek te gaan ??

Dat vraagt transparantie en bereidheid



Spanningsveld

Investeren in leveranciersrelatie



Europees aanbestedingsrecht



Wat is realistisch

Cybersecurity intake

- *Classificeer de dienst*
 - Business impact analyse
- *Bepaal belang leverancier*
 - Stel TIER-level vast
- *Maak passend eisenpakket*
 - Proces, technisch en volwassenheid
- *Borging in contract management*
 - Walk the talk

Belang	Business impact	Toegang tot gegevens	Werken aan systemen	Verplichtingen in de wet- en regelgeving	
Hoog (Tier 1)	Advanced	Niveau be pad	Advanced / Volwassenheidsniveau A1	Advanced / Volwassenheidsniveau A2	Advanced / Volwassenheidsniveau A3
Midden (Tier 2)	Intermediate		Intermediate / Volwassenheidsniveau I1	Intermediate / Volwassenheidsniveau I2	Intermediate / Volwassenheidsniveau I3
Laag (Tier 3)	Basic		Basic / Volwassenheidsniveau B1	Basic / Volwassenheidsniveau B2	Basic / Volwassenheidsniveau B3



Kwaliteit boven kwantiteit

Entry t/m Advanced



Hoeveel te nemen maatregelen

Kwantiteit

Volwassenheid



Hoe goed doet de organisatie het

Kwaliteit

Wat is belangrijker, de hoeveelheid of de zorgvuldigheid

CYRA-OT - Entry

0 van de 32 vragen beantwoord

Assessment afronden >

🔍 worden remote



Alle vragen Per categorie Per niveau

NET 3.3 SR 2.6 **Worden remote sessies beëindigd na een vastgestelde tijd?**

🔄 Open

Antwoord: Ja

Worden remote sessies beëindigd na een vastgestelde tijd?

Onderwerp: Remote access termination Remote session termination

Norm: IEC 62443-2-1 IEC 62443-3-3

Beheersmaatregel: NET 3.3 SR 2.6

Niveau: Entry

Selecteer wat van toepassing is

- Ja
- Nee
- Niet van toepassing

Volwassenheid

- Level 1** | De remote sessies worden na een vaste tijdsperiode (van inactiviteit) automatisch beëindigd. Dit is niet vastgelegd in beleid of procedures.
- Level 2** | In beleid en/of procedures is vastgelegd dat na een bepaalde tijdsperiode en onder vastgestelde voorwaarden de remote sessie automatisch wordt beëindigd.
- Level 3** | In beleid en/of procedures is vastgelegd na welke tijdsperiode en onder welke voorwaarden de remote sessie automatisch wordt beëindigd. OT-systemen worden periodiek getoetst of ze voldoen aan het beleid of de procedure en gecorrigeerd waar nodig.

Bewijs - verplicht

Licht je antwoord toe met een onderbouwing.

CYRA-OT - Advanced

0 van de 103 vragen beantwoord

Assessment afronden >

rolgebaseerde



Alle vragen

Per categorie

Per niveau

USER Hoe is rolgebaseerde toegang ingericht voor het OT-domein?

1.5
SR
2.
1
RE(2)

Open

Antwoord: Ja

Hoe is rolgebaseerde toegang ingericht voor het OT-domein?



Onderwerp: Least privilege Authorization enforcement - Permission mapping to roles

Norm: IEC 62443-2-1 IEC 62443-3-3

Beheersmaatregel: USER 1.5 SR 2.1 RE(2)

Niveau: Advanced

Selecteer wat van toepassing is

- Ja
- Nee
- Niet van toepassing

Volwassenheid

- Level 1** | In de praktijk is rolgebaseerde toegang beperkt ingericht voor enkele OT-gebruikers. Rollen en toegangsrechten zijn deels bekend binnen het team, maar niet formeel vastgelegd. beleid en/of procedures waarin rollen, rechten en hun toepassing zijn beschreven, ontbreken.
- Level 2** | In beleid en/of procedures is vastgelegd dat rolgebaseerde toegang wordt toegepast en dat is beschreven welke toegangsrechten de beschreven rollen krijgen.
- Level 3** | In beleid en/of procedures is vastgelegd dat rolgebaseerde toegang wordt toegepast en dat is beschreven welke toegangsrechten de beschreven rollen krijgen. Periodiek wordt het beleid of de procedure gecontroleerd tegen de werkelijk uitgegeven toegangsrechten en gecorrigeerd waar nodig.

Bewijs - verplicht

Licht je antwoord toe met een onderbouwing.



*“Volwassen leveranciersmanagement in OT gaat niet over het vermijden van afhankelijkheden,
maar over het aantoonbaar beheersen ervan”*



Stelling 1

OT-security is binnen onze organisatie nog steeds vooral een IT-feestje



Stelling 2

Wij kennen de belangrijkste risico's van onze leveranciers met een OT-omgeving



Stelling 3

In onze OT-omgeving is beschikbaarheid belangrijker dan security – en dat blijft zo



Stelling 4

De verantwoordelijkheden zijn tussen ons en onze stakeholders goed verdeeld



Stelling 5

Hoe bepalen jullie de relevante security-eisen voor een leverancier?



Bedankt voor jullie aandacht!

Wil je meer weten over de CYRA-methode?

hetccv.nl/cyra

