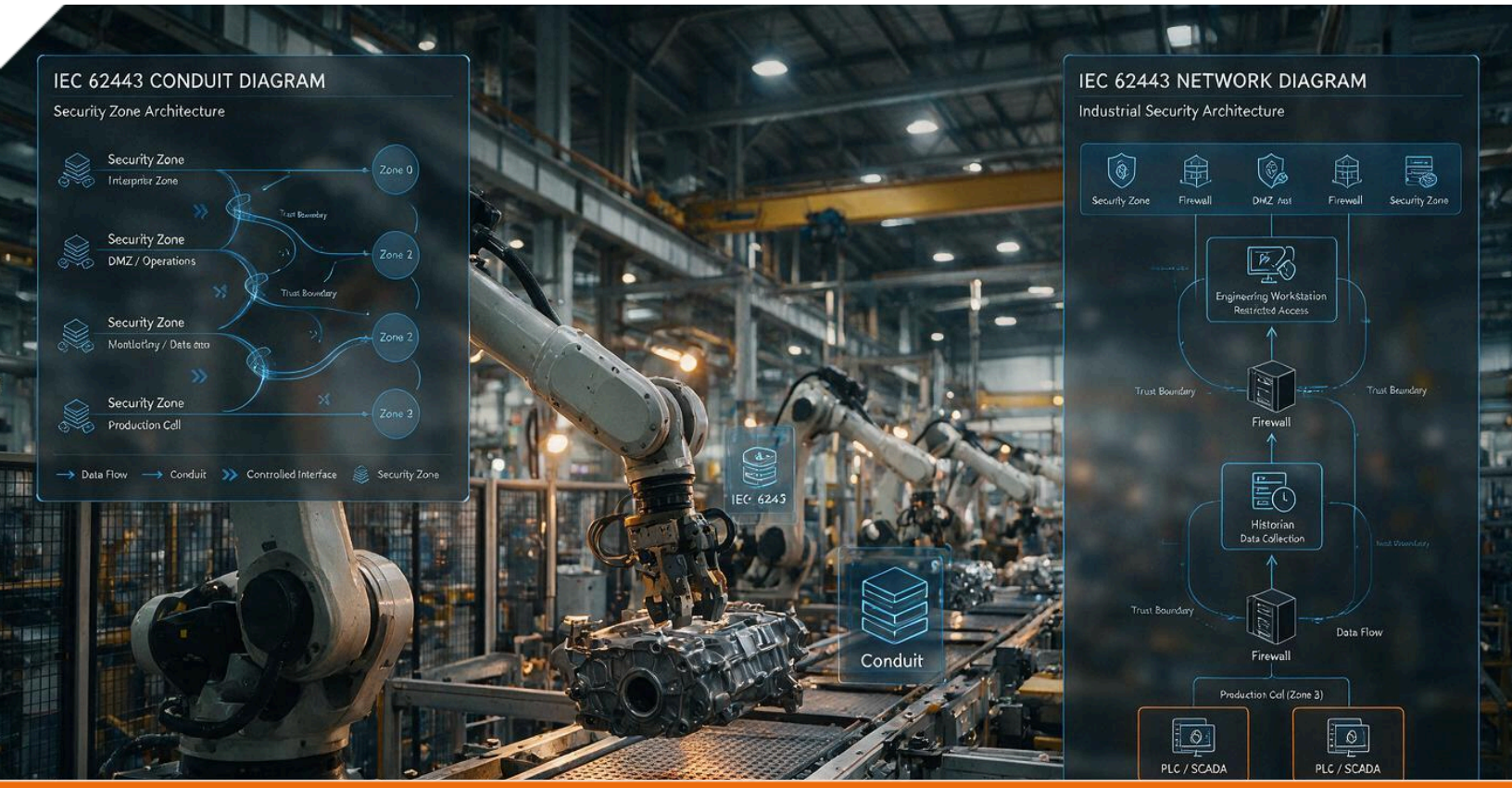
IEC 62443 Architectuurcheck

Zones, conduits & noodzakelijke dataflows

10 praktische vragen voor OT-architectuur

Versie 1.0



CYBERBUSTERS B.V.

Hoe gebruik je deze check?

Leg je huidige OT-architectuur of netwerkdiagram voor je.
Beantwoord elke vraag met:

- Ja = 2 punten
- Deels = 1 punt
- Nee = 0 punten

De 10 praktische vragen

Vraag	Antwoordopties	Score
1. Is het System under Consideration duidelijk afgebakend? Check: Weten we precies wat binnen en buiten de scope valt?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
2. Kunnen we uitleggen waarom systemen in dezelfde zone zijn gegroepeerd? Check: Is de groepering gebaseerd op functie, risico en beschermingsbehoefte in plaats van historie of VLAN-structuur?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
3. Zijn IT en OT bewust van elkaar gescheiden? Check: Weten we welke communicatie tussen beide echt nodig is en waarom?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
4. Zijn safety-gerelateerde functies bewust gescheiden? Check: Zijn noodzakelijke verbindingen met andere zones bekend en beperkt?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
5. Zijn de noodzakelijke dataflows tussen zones in kaart gebracht? Check: Kennen we bron, bestemming, richting, doel en operationele noodzaak van elke belangrijke flow?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
6. Kunnen we uitleggen waarom elke belangrijke dataflow nodig is? Check: Kunnen we het operationele doel beschrijven, niet alleen de firewall- of netwerkregel?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
7. Weten we welk beschermingsniveau nodig is voor elke relevante zone en conduit? Check: Is het gewenste beschermingsniveau afgeleid van risico, in plaats van overal hetzelfde toegepast?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	

Vraag	Antwoordopties	Score
8. Is externe en leverancierstoegang zichtbaar en beheerst? *Check: Weten we wat leveranciers kunnen bereiken, wanneer toegang is toegestaan en hoe deze kan worden ingetrokken?*	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
9. Weten we wat er gebeurt als een belangrijke verbinding niet beschikbaar is? *Check: Kunnen we een verbinding isoleren zonder een onverwacht operationeel of safety-probleem te veroorzaken?*	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
10. Kan elke bestaande communicatiestroom worden onderbouwd? Check: *Zijn legacyverbindingen en tijdelijke uitzonderingen beoordeeld en gekoppeld aan een actuele operationele noodzaak?*	Ja = 2 pt Deels = 1 pt Nee = 0 pt	

Jouw resultaat

- **17–20 punten (Goed onderbouwde architectuur):** Je architectuur toont een sterke risicogedreven basis. Zones, noodzakelijke dataflows, externe toegang en beschermingsbehoeften zijn grotendeels te verklaren vanuit operationele eisen en risico.
  Volgende stap: valideer dat de architectuur actueel, gedocumenteerd en met bewijs onderbouwd is. Beoordeel wijzigingen, leverancierstoegang en gewenste security levels periodiek.
- **11–16 punten (Architectuur heeft verdere onderbouwing nodig):** De basisstructuur is aanwezig, maar sommige ontwerpkeuzes zijn nog niet volledig begrepen, gedocumenteerd of aan risico gekoppeld.
  Volgende stap: begin met elke vraag die met Deels of Nee is beantwoord. Bepaal de ontbrekende risico-onderbouwing, noodzakelijke dataflow, eigenaar of beveiligingseis.
- **0–10 punten (Architectuurreview aanbevolen):** Belangrijke architectuurkeuzes kunnen nog onvoldoende worden verklaard vanuit risico en operationele noodzaak.
  Volgende stap: ga terug naar de basis. Definieer het System under Consideration, beoordeel het zonemodel, identificeer noodzakelijke dataflows en externe toegang en bepaal de vereiste bescherming voordat je meer technische maatregelen toevoegt.

Ongeacht de totaalscore verdient een Nee op een van de volgende punten prioriteit:

- System under Consideration is onduidelijk
- noodzakelijke dataflows zijn onbekend
- SL-T / vereiste bescherming is niet risicogebaseerd
- externe of leverancierstoegang is onduidelijk
- operationele impact van het wegvallen van een verbinding is onbekend

Disclaimer: Deze Architectuurcheck is een praktisch screeningsinstrument en toont geen IEC 62443-compliance aan en vervangt geen formele beoordeling of audit.

Vragen over jouw resultaat? Neem gerust contact op: https://cyber-busters.com/contact