Co-funded by
the European Union

Cyber-In

Inleiding tot OT-cyberbeveiliging voor docenten

29 januari 2026

2023-1-NL01-KA220-VET-000153812

Co-funded by
the European Union

Cyber-In

Leerresultaten

- Ervaar cyberdreigingen in een OT-context door middel van begeleide simulaties.
- Pas OT-cyberbeveiligingsstrategieën toe in gesimuleerde scenario's.
- Ontwikkel vaardigheden op het gebied van incidentbeheer en crisiscommunicatie.

Co-funded by
the European Union

Cyber-In

Inleiding tot OT-omgevingen

Inzicht in operationele technologie in industriële contexten

Co-funded by
the European Union

Cyber-In

Wat is operationele technologie (OT)?

- OT verwijst naar hardware en software die fysieke apparaten en processen bewaakt en bestuurt.
- Veelvoorkomend in sectoren zoals productie, energie, water en transport.
- De focus ligt op beschikbaarheid, veiligheid en realtime-operaties.

Co-funded by
the European Union

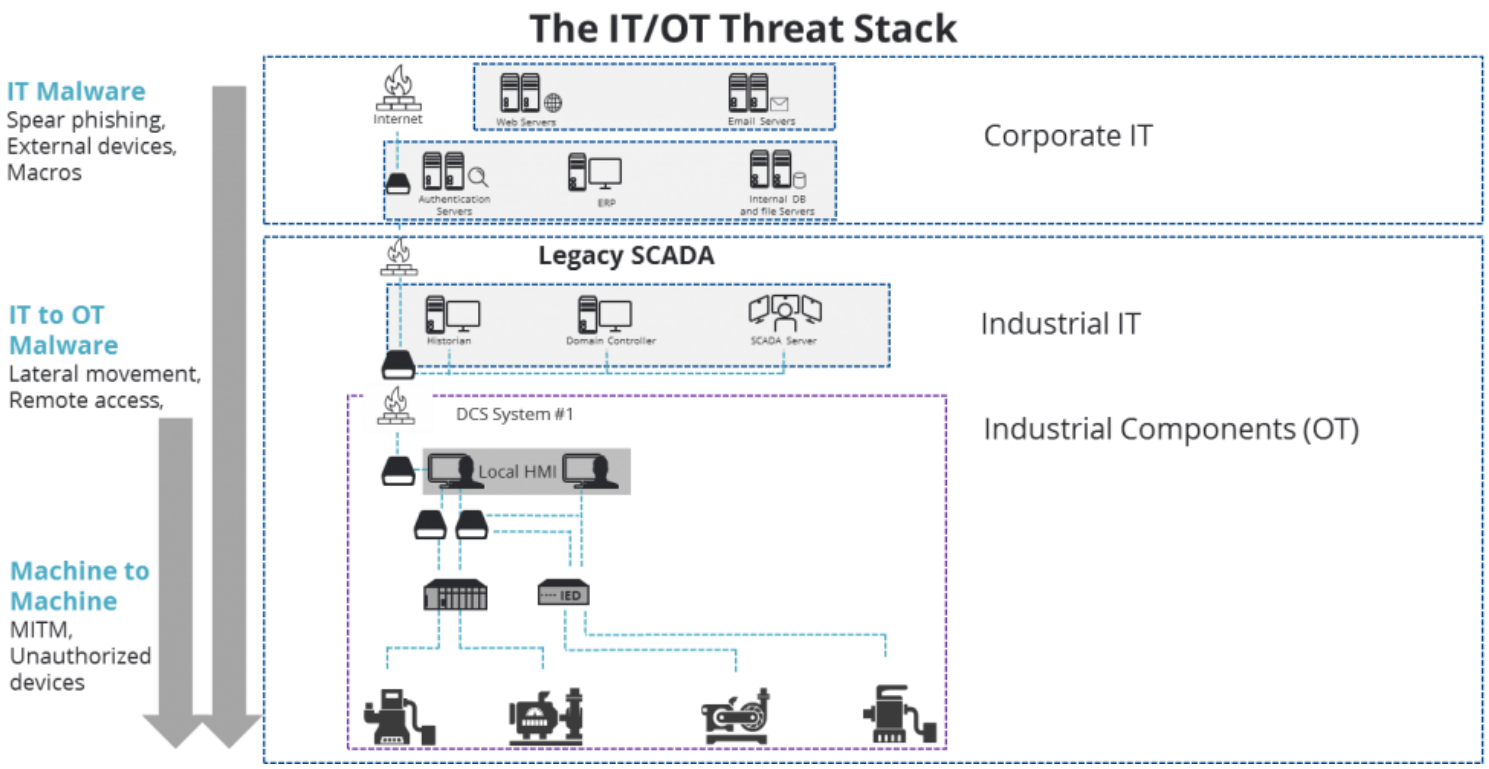
Cyber-In

OT versus IT – Belangrijkste verschillen

- Aspect | OT | IT
- Hoofddoel | Fysieke procesbesturing | Gegevensverwerking en -beheer
- Prioriteiten | Veiligheid, beschikbaarheid, realtime | Vertrouwelijkheid, integriteit, beschikbaarheid
- Omgeving | Industrieel | Kantoren
- Update-cycli | Zelden | Regelmatig
- Apparaten | PLC's, sensoren, actuatoren | Servers, laptops

Co-funded by
the European Union

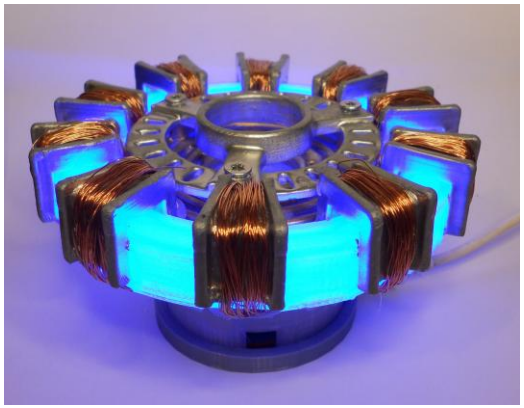
Cyber-In



Co-funded by
the European Union

Cyber-In

Prioriteiten van OT versus IT



- OT geeft prioriteit aan beschikbaarheid en operationele continuïteit.
- IT geeft prioriteit aan de vertrouwelijkheid en integriteit van gegevens.
- OT-systemen moeten veilig blijven draaien, terwijl IT-systemen gevoelige informatie beschermen

Co-funded by
the European Union

Cyber-In

Belangrijke OT-componenten

- PLC: Voert de besturingslogica voor machines en processen uit.
- SCADA: Gecentraliseerd systeem voor gegevensverzameling en besturing.
- HMI: Interface die interactie tussen mens en machine mogelijk maakt.
- RTU: Verzamelt gegevens en stuurt deze naar SCADA.

Co-funded by
the European Union

Cyber-In

De rol van OT-componenten in een industrieel systeem

- PLC's regelen processen zoals transportbanden.
- HMI's geven de machinestatus weer.
- RTU's verbinden externe locaties met het controlecentrum.
- SCADA biedt gecentraliseerd inzicht en controle.

Co-funded by
the European Union

Cyber-In

Het Purdue-model

- Niveau 0: Fysiek proces (sensoren, actuatoren)
- Niveau 1: Besturing (PLC's)
- Niveau 2: Toezicht (SCADA, HMI's)
- Niveau 3: Bedrijfsvoering (productiebeheer)
- Niveau 4: Bedrijfsvoering (ERP, IT-systemen)

Co-funded by
the European Union

Cyber-In

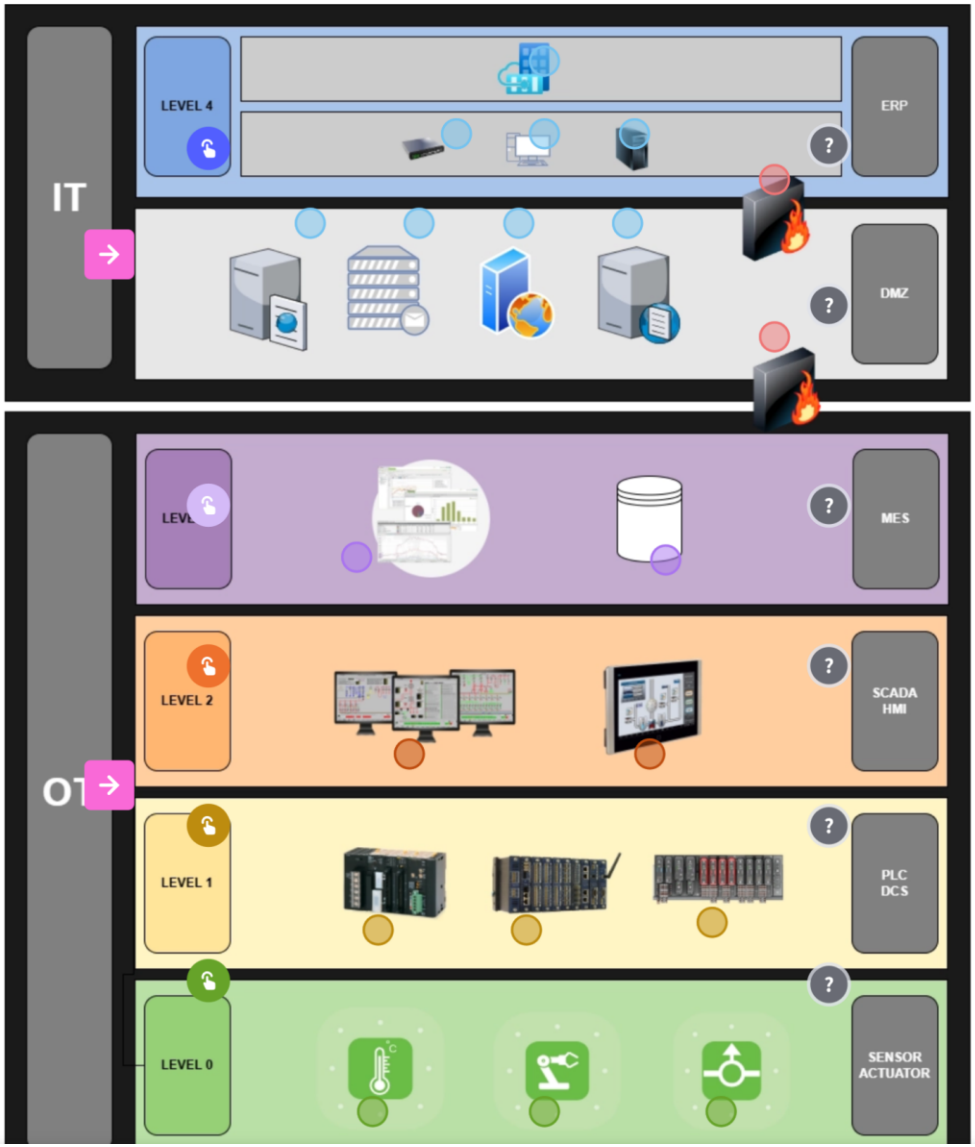
Beveiligingslagen in het Purdue-model

- Segmentatie is essentieel: isoleer niveaus om risico's te verminderen.
- Een diepgaande verdedigingsaanpak:
  - Firewalls tussen IT en OT
  - Netwerksegmentatie en VLAN's
  - Monitoring- en inbraakdetectiesystemen
  - Op rollen gebaseerde toegangscontrole (RBAC)

Co-funded by
the European Union

Cyber-In

CYBER-IN ARCHITECTURE



Co-funded by
the European Union

Cyber-In

Aandachtspunten

- OT richt zich op realtime fysieke activiteiten.
- Belangrijkste componenten: PLC's, SCADA, HMI, RTU's.
- Het Purdue-model structureert en beveiligt OT-omgevingen.
- Inzicht in OT is cruciaal voor de bescherming van kritieke infrastructuur.

Co-funded by
the European Union

Cyber-In

Verschillen op het gebied van cyberbeveiliging: OT versus IT

Inzicht in de specifieke uitdagingen op het gebied van operationele technologie en informatietechnologie

Co-funded by
the European Union

Cyber-In

Verschillen in de gevolgen

- Cyberincidenten op het gebied van OT kunnen leiden tot lichamelijk letsel of veiligheidsrisico's.
- Bij IT-inbreuken gaat het doorgaans om gegevensdiefstal of schendingen van de privacy.
- De gevolgen van OT-aanvallen kunnen directer en gevaarlijker zijn.

Co-funded by
the European Union

Cyber-In

Unieke OT-kwetsbaarheden

- Oude systemen met beperkte beveiligingsupdates.
- Gebrek aan versleuteling of authenticatie.
- Fysieke toegang staat vaak gelijk aan toegang tot het systeem.
- Protocollen die niet zijn ontworpen met het oog op cyberbeveiliging (bijv. Modbus, DNP3

Co-funded by
the European Union

Cyber-In

Praktijksessie

Co-funded by
the European Union

Cyber-In

Agenda

- In groepen bespreken.
- Scenario's kiezen.
- Presenteer oplossingen.

Co-funded by
the European Union

Cyber-In

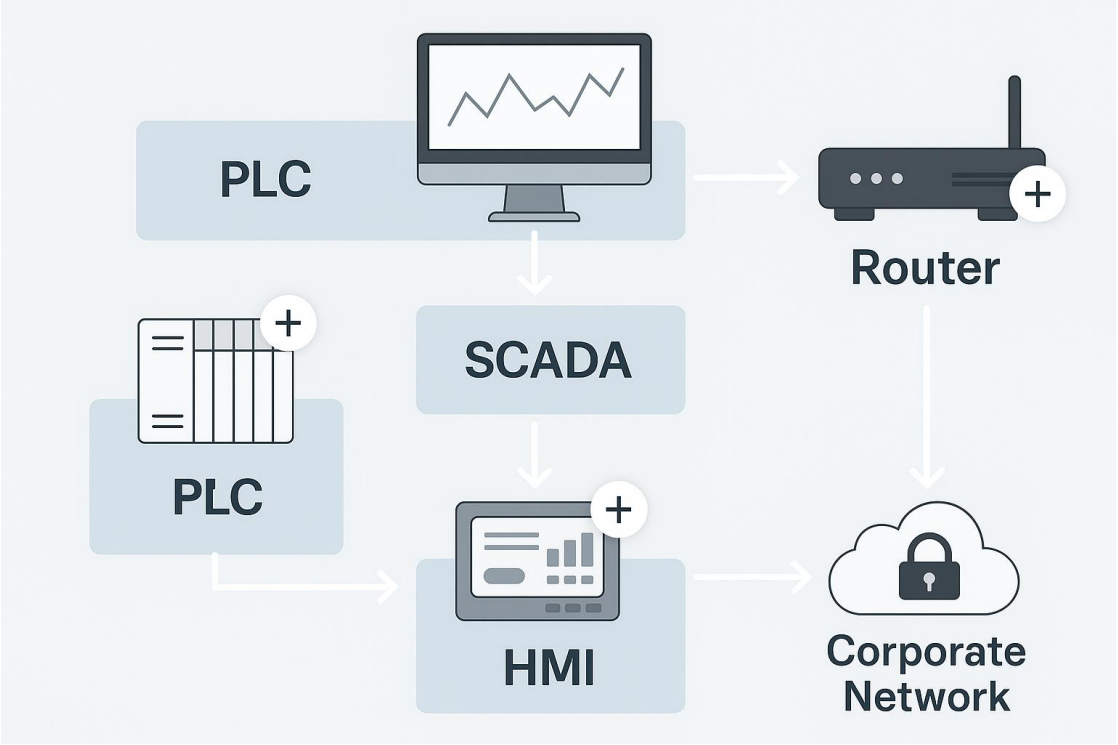
Scenario 1

- Een ransomware-aanval verstoort de pompbesturing in een OT-netwerk. Deelnemers zullen:

Co-funded by
the European Union

Cyber-In

Scenario 1



Co-funded by
the European Union

Cyber-In

Scenario 1: Tijdlijnkaarten

- 09:00 - Operators melden afwijkende waarden op de HMI
- 09:10 - Pompen reageren niet meer op SCADA-opdrachten
- 09:20 - Er verschijnt een losgeldbrief op het engineeringwerkstation
- 09:30 - Piek in netwerkverkeer naar onbekend IP-adres gedetecteerd

Co-funded by
the European Union

Cyber-In

Scenario 1: Opdrachtinstructies

- Wat doe je nu?
- Wie breng je op de hoogte?
- Hoe isoleer je de getroffen componenten?
- Welke maatregelen kun je nemen om de gevolgen te beperken?

Co-funded by
the European Union

Cyber-In

Scenario 2

- Een vermoedelijke bedreiging van binnenuit leidt tot een wijziging in de PLC-configuratie, wat een productieafwijking veroorzaakt.
  Deelnemers zullen:

Co-funded by
the European Union

Cyber-In

Scenario 2 Tijdlijnkaarten:

- 08:45 - Een PLC wordt bijgewerkt via de USB-poort
- 09:00 - De productielijn stopt onverwacht
- 09:10 - Uit onderzoek blijkt dat er ongeautoriseerde logica is geüpload
- 09:20 - Logbestanden van het USB-apparaat tonen toegang door een onbekende gebruiker

Co-funded by
the European Union

Cyber-In

Scenario 2: Opdrachten

- Hoe controleert u de wijziging?
- Hoe onderzoek en beperk je het probleem?
- Welke controles hebben gefaald?
- Welk langetermijnbeleid moet worden aangepast?

Co-funded by
the European Union

Cyber-In

Scenario 2: Opdrachten

- Hoe controleert u de wijziging?
- Hoe onderzoek en beperk je het probleem?
- Welke controles hebben gefaald?
- Welk langetermijnbeleid moet worden aangepast?

Co-funded by
the European Union

Cyber-In

Scenario 2: Opdrachten

- Hoe controleert u de wijziging?
- Hoe onderzoek en beperk je het probleem?
- Welke controles hebben gefaald?
- Welk langetermijnbeleid moet worden aangepast?

Co-funded by
the European Union

Cyber-In

Scenario 3: Rollenspel over crisisrespons

Groepen en rollen:

- Team 1: OT-manager
- Team 2: Hoofd IT-beveiliging
- Team 3: PR-medewerker

Co-funded by
the European Union

Cyber-In

Scenario 3: Rollenspel over crisisrespons

- **Achtergrond**: U speelt de rol van [rol], en de faciliteit is gedeeltelijk stilgelegd als gevolg van een cyberaanval.
- **Doelstelling**: De respons coördineren, de uitvaltijd tot een minimum beperken en de reputatie beschermen.

Co-funded by
the European Union

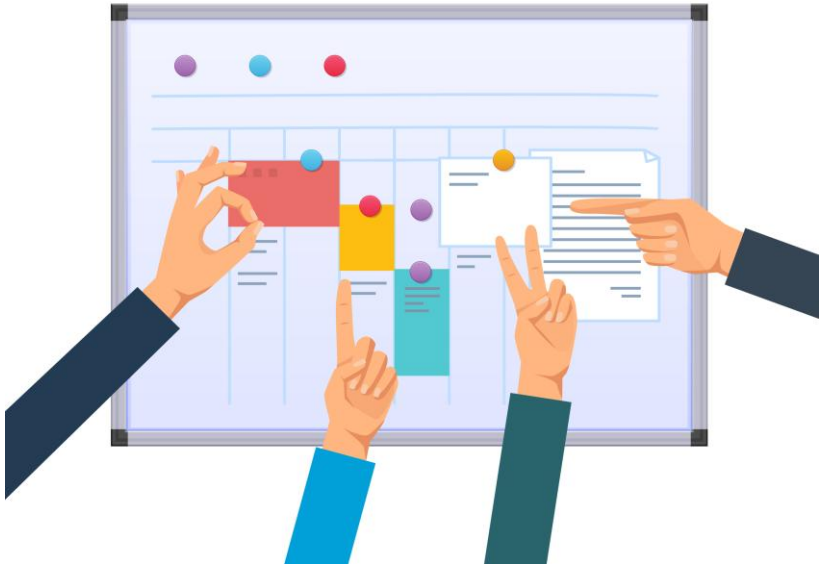
Cyber-In

Scenario 3: Taken

- Bepaal uw prioriteiten (bijv. veiligheid, gegevensintegriteit, reactie in de media)
- Bereid een teambriefing van 2 minuten voor
- Beantwoord 2 vragen van belanghebbenden die door de facilitator worden gesteld

Co-funded by
the European Union

Cyber-In



Interactieve discussie

Open vragen en brainstormen

Co-funded by
the European Union

Cyber-In

Open vragen ter overweging

- Wat zijn de grootste uitdagingen op het gebied van cyberbeveiliging waarmee u in uw werk te maken hebt gehad?
- Hoe gaat uw organisatie momenteel om met OT-beveiliging?
- Zijn er specifieke kwetsbaarheden die je herhaaldelijk bent tegengekomen?

Co-funded by
the European Union

Cyber-In

Ervaringen delen

- Deel een incident of bijna-ongeval uit het verleden waarbij OT-systemen betrokken waren.
- Welke lessen zijn hieruit getrokken?
- Hoe heeft uw team gereageerd of zich aangepast?

Co-funded by
the European Union

Cyber-In

Oplossingen bedenken

- Welke goedkope of zeer effectieve verbeteringen kunnen worden doorgevoerd op het gebied van OT-beveiliging?
- Hoe kan de samenwerking tussen IT en OT worden verbeterd?
- Wat voor soort training zou OT-medewerkers helpen om meer cyberbewust te worden?

Co-funded by
the European Union

Cyber-In

Bedankt!

- Bedankt voor jullie inbreng en betrokkenheid!
- Laten we het gesprek voortzetten en ideeën blijven uitwisselen.