



Ministerie van Infrastructuur
en Waterstaat

Secura Training OT Cybersecurity Professional Training

Industriële controlesystemen (ICS) zijn onmisbaar voor een vlot en veilig verloop van het dagelijks leven. Ze ondersteunen alles, van kritieke infrastructuur tot gebouwbeheer. Met de juiste kennis en expertise houden we deze systemen cyberweerbaar.

Daarom organiseert het cybersecuritybedrijf Secura de OT Cybersecurity Professional Training als vervolg op de OT Cybersecurity Fundamentals Training. In deze flyer lees je over de meerwaarde en inhoud van deze training en hoe je je kunt aanmelden.

Voor wie is de OT Cybersecurity Professional Training?

Deze tweedaagse training is voor professionals met een basiskennis van OT-cybersecurity, zoals besturingssystemingenieurs, IT- en OT-beveiligingspersoneel en managementprofessionals. Het is handig om eerst de OT Fundamentals Training te volgen. Daarnaast is kennis over OT-cybersecurity wel aanbevolen. Denk aan kennis over netwerktechnologieën, het Purdue-model, risicomethodologie, dreigingsactoren, dreigingsmodellering en fundamentele beveiligingsprincipes zoals CIA-triad, toegangscontrole, firewalls, logging en antivirus.



Programma
**Versterken
Cyberweerbaarheid
in de watersector**



Programma
**Versterken Cyberweerbaarheid
in de Luchtvaart- en Maritieme
sector**



Programma
**Versterken Cyberweerbaarheid
in de Weg- en Spoorvervoer
sectoren**

Wat kun je van de training verwachten?

- Herhaal belangrijke informatie uit de OT Fundamentals Training.
- Krijg basisbegrip van netwerken, encryptie en OT-netwerkarchitecturen.
- Krijg volledig begrip van het ICS-landschap: industriële processen, kaders, beleidslijnen, risico's en protocollen.
- Leer over IEC62443- en NIST CSF-kaders, cybersecurityprogramma's en risicobeoordelingen in OT.
- Ontdek OT-cybersecurityuitdagingen en de verschillen met IT-omgevingen.
- Leer firewalls in ICS-netwerken toepassen.
- Leer verschillende besturingsystemen (OS) kennen en hoe deze te versterken.
- Krijg inzicht in fysieke beveiliging van een ICS-faciliteit.
- Krijg inzicht in antivirus- en eindpuntbeschermingsuitdagingen in ICS-netwerken en OT-systeem patching.
- Leer ICS-netwerken verdedigen met logging, monitoring en Incident Response.
- Krijg inzicht in OT-assetinventaris en back-ups voor OT-systemen.



Wat houdt de training in?

Het programma is verdeeld in vier modules, gegeven in een tweedaagse training. Nadat je de training hebt voltooid krijg je een certificaat.

Dag 1

Module 1: Inleiding & herhaling OT Fundamentals

Deze module behandelt:

- basisprincipes van ICS: terminologie, industriële processen, regeltheorie, plantorganisatie en herhaling van de OT Fundamentals Training;
- basiskennis over netwerkprincipes, inclusief het OSI-model;
- basiskennis van draadloze netwerken, draadloze ICS-protocollen en kwetsbaarheden;
- een inleiding tot cryptografie: symmetrische en asymmetrische cryptografie, hash-algoritmen en MAC's.

Module 2: ICS-protocollen, componenten en veilige ICS-netwerkarchitectuur

Je leert in deze module over:

- veelgebruikte industriële protocollen in ICS-netwerken;
- het ontwerpen van veilige ICS-netwerkarchitecturen door segmentatie, netwerkgrenzen, firewalls, datadiodes en industriële IDS;
- het ICS-aanvalsoppervlak, technieken voor categoriseren van aanvallen, aanvalsbomen en dreigingsmodellen;
- het in kaart brengen en onderzoeken van relevante ICS-aanvallen op elk Purdue-niveau.

Dag 2

Module 3: Cyber Security Programma's

Deze module gaat over:

- het opzetten van een cybersecurityprogramma voor ICS-netwerken met IEC62443- en NIST CSF-kaders;
- het ontwikkelen van documentatie, inclusief beleid en procedures;
- het uitvoeren van risicobeoordelingen om potentiële bedreigingen en kwetsbaarheden te identificeren.

Module 4: Beveiligingsmaatregelen

Bij de vierde module leer je:

- een uitgebreide ICS-assetinventaris en fysieke beveiligingsmaatregelen op te stellen;
- besturingsystemen en eindpuntbeschermingsoplossingen te versterken;
- hoe je patchmanagement voor OT-systemen en systeemback-ups kunt implementeren;
- over logging en monitoring binnen ICS-netwerken en incidentresponstrategieën.

Aanmelden

Wil je een OT Cybersecurity Professional Training voor jouw organisatie? Stuur dan een e-mail naar:



De watersector:

cyberweerbaarheidwater@minienw.nl



De luchtvaart- of maritieme sector:

cyberweerbaarheidluchtvaartmaritiem@minienw.nl



De weg- of spoorvervoersector:

cyberweerbaarheidweg-spoorvervoer@minienw.nl