Ministerie van Infrastructuur
en Waterstaat

Secura Training

OT Cybersecurity Fundamentals Training

Operationele Technologie (OT) is de laatste jaren een steeds groter doelwit geworden van cyber-aanvallen van criminelen en statelijke actoren.

Maar met de juiste kennis en expertise verklein je het risico op cyberaanvallen. Eind dit jaar organiseert het gerenommeerde cybersecuritybedrijf Secura tweedaagse trainingen in Cyberbeveiliging voor OT. 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 Fundamentals Training?

De OT Cybersecurity Fundamentals Training is interessant voor bestuurders, assetmanagers, technisch en functioneel beheerders, besturingssysteemingenieurs en IT- en OT-beveiligingspersoneel. Maar omdat de training is ontworpen als een algemene kennismaking met OT-cybersecurity, kan iedereen met interesse in OT en techniek meedoen. Basiskennis van computers, netwerken en beveiligingsprincipes is wel aanbevolen.

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 houdt de training in?

Deze tweedaagse training geeft je inzicht in het ICS-beveiligingslandschap. Industriële besturingssystemen (ICS), zoals kritieke infrastructuur en gebouwautomatisering, zijn de ruggengraat van ons dagelijks leven. Als deelnemer leer je deze systemen te beoordelen en verdedigen.

Dag 1

Module 1: Inleiding tot ICS

De eerste trainingsdag start met een overzicht van ICS-fundamenten. Tijdens deze aftrap raak je bekend met alle relevante begrippen en leer je het ICS-beveiligingslandschap kennen.

Deze module behandelt:
- basisbegrippen en industriële processen;
- de verschillen tussen IT en OT;
- de potentiële cyberimpact in de OT-omgeving;
- de werking van een regelkring in een laboratorium-omgeving;
- de geschiedenis van ICS-beveiliging.

Module 2: ICS-componenten en architectuur

Tijdens de tweede module duik je in het Purdue-model en alle componenten van typische ICS-netwerken. Zo leer je meer over de architectuur van deze systemen en de kwetsbaarheden.

Je maakt kennis met:
- instrumenten, Programmable Logic Controllers (PLCs) en veiligheidscontrollers;
- de veelvoorkomende cyberzwakheden van typische ICS-netwerken;
- de netwerkcomponenten, industriële protocollen en netwerkarchitecturen;
- de kwetsbaarheden van ICS-apparatuur aan de hand van voorbeelden en lab-demonstraties. Dit doe je met behulp van een OT Box: een demomedium bestaande uit huidige ICS-apparatuur.

Dag 2

Module 3: ICS-dreigingen, cyberfysieke aanvallen en aanvalsoppervlak

Na een korte samenvatting van dag 1 leer je vervolgens meer over ICS-dreigingen. Hier staan de motieven en capaciteiten van aanvallers centraal. Ook behandel je de impactfactoren bij het goed beoordelen van cyberrisico's.

Deze module behandelt:
- complexe aanvallersactiviteiten zoals gerichte industriële spionage en destructieve cyberfysieke aanvallen;
- procesbegrip en het ontwerp van schadescenario's om mogelijke cyberfysieke impact te analyseren;
- het uitgebreide aanvalsoppervlak van industriële besturingssystemen.

Tijdens interactieve discussies leer je typische OT-beveiligingsproblemen te herkennen én te verhelpen of verlichten.

Module 4: Beveiligingsnormen, dreigingsmodellering en actuele casestudy's

In module 4 staat het toepassen van de opgedane kennis centraal. Je leert hoe je effectieve beveiligingsmaatregelen treft en risico's beheert.

Dit doe je door:
- te kijken naar een ICS-omgeving door de ogen van een aanvaller;
- alle aanvalsvectoren in de eerder genoemde OT Box te vinden
- actuele casestudy's te analyseren en bekende incidenten te bespreken.

Waarom deelnemen aan de training?

Meedoen aan de training geeft je waardevolle inzichten in je ICS-beveiliging. Je raakt vertrouwd met beveiligingsuitdagingen en leert veelvoorkomende kwetsbaarheden op te sporen. Zo vergroot je de cyberweerbaarheid van jouw bedrijf en verklein je het risico op destructieve aanvallen.

Aanmelden

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

Watersector:
cyberweerbaarheidwater@minienw.nl

De luchtvaart- of maritieme sector:
cyberweerbaarheidluchtvaartmaritiem@minienw.nl

De weg- of spoorvervoersector:
cyberweerbaarheidweg-spoorvervoer@minienw.nl