SIEMENS

Hands-on workshop Industrial Security (WS-I-SEC)

Korte beschrijving

Industrial Security
Hoe beveiligt u uw productieomgeving optimaal tegen cyberaanvallen en geeft u hackers geen kans? Wat zijn de mogelijkheden van TIA Portal en Siemens' SCALANCE gamma op het vlak van beveiliging? En hoe zorgt u ervoor dat de voordelen van automatisering niet ten koste gaan van uw bescherming?
De workshop
Het antwoord op al deze vragen ontdekt u tijdens de hands-on workshop Industrial Security. We gaan kort in op de nieuwe NIS-wetgeving en onze security assesment services komen ook aan bod. U leert er onder meer de verschillende beveiligingsmogelijkheden van TIA Portal en SCALANCE kennen. Zowel het automatisatienetwerk als de componenten (PLC en visualisatie) komen aan bod. Naast de hardware biedt Siemens ook de mogelijkheid aan klanten om hun huidig netwerk te onderzoeken en te challengen op security (analyse, identificeren van zwakheden, beschikbare oplossingen).
Ontdek hoe u uw productieomgeving optimaal tegen cyberaanvallen beschermt met TIA Portal en SCALANCE in deze hands-on workshop.

Doelen

Recente evoluties zoals remote control, 'digital twins' en open standaarden zorgen voor heel wat nieuwe mogelijkheden. Tegelijkertijd maken ze productieomgevingen ook kwetsbaarder voor cyberaanvallen.
Tijdens de workshop verkennen we beveiliging op drie niveau's: systeemintegriteit, netwerkbeveiliging en fysieke beveiliging. We baseren ons daarbij op de wereldwijde ISA 99/IEC 62443-standaard voor industriële automatisatie.
Ook gaan we dieper in op de verschillende beveiligingsmogelijkheden binnen TIA Portal en het SCALANCE gamma. Na de sessie beschikt u over heldere best practices voor het beveiligen van zowel automatisatienetwerken als componenten.

Inhoud

- **De NIS-richtlijn en het Defense-in-Depth-concept (theorie)**

Wat houdt de NIS-richtlijn – de eerste EU-wetgeving over cybersecurity – precies in, en wat betekent ze voor u? En wat zijn de principes achter het 'defense-in-depth'-concept? Het antwoord krijgt u in deze sessie.

- **Systeemintegriteit (theorie + praktijk)**

Siemens' geïntegreerde beveiligingsfeatures bieden optimale bescherming tegen een brede waaier aan bedreigingen: van het kopiëren van configuratiedata tot het manipuleren van bestanden.

- **Netwerkbeveiliging (theorie + praktijk)**

Van netwerkbeveiligingsmanagement en netwerksegmentatie tot gecodeerde communicatie: hoe beschermt u uw automatiseringsnetwerken tegen ongeautoriseerde toegang? Ontdek hoe Siemens Professional Services u kunnen helpen.

- **Fysieke beveiliging (theorie)**

Beveiliging op fabrieksniveau begint bij fysieke toegangscontrole en het afschermen van gevoelige zones met keycards. Het startpunt voor bescherming op maat is steeds een uitgebreide risicoanalyse, gevolgd door implementatie en nauwkeurige monitoring.

Vereiste voorwaarden

Basiskennis van TIA Portal is vereist. Bij inschrijvingen in groepen van twee personen volstaat het dat één iemand over de nodige expertise beschikt.

Opmerking

8u30 – Verwelkoming
9u00
– NIS-wetgeving en het Defense-in-Depth-concept
– Systeemintegriteit: deel I
– Koffiepauze
– Systeemintegriteit: deel II
12u30 – Lunch
13u15
– Netwerkbeveiliging
– Fysieke beveiliging
– Koffiepauze
– Netwerkbeveiliging
16u45 – Feedback en conclusies

Soort

Face-to-face-training

Duur

1 dag

Taal

nl