

Opleiding : ISO/IEC 62443: inzicht in de cyberbeveiliging van industriële systemen

Praktijkcursus - 2d - 14u00 - Ref. SYI

Prijs : 1760 € V.B.

NEW

Een intensieve training om de basisprincipes van de norm ISO/IEC 62443 te begrijpen, de terminologie en de belangrijkste concepten (zones en kanalen, beveiligingsniveaus, fundamentele eisen) onder de knie te krijgen en te leren hoe de norm in de praktijk op een industrieel systeem kan worden toegepast aan de hand van begeleide casestudies

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- ✓ Inzicht krijgen in de uitdagingen op het gebied van cyberbeveiliging van industriële systemen (OT/ICS) en hun specifieke kenmerken ten opzichte van IT
- ✓ Inzicht krijgen in de structuur van de ISO/IEC 62443-normenreeks en de rol van elk van de documenten daarin
- ✓ Een vereenvoudigde risicoanalyse uitvoeren en een indeling in zones en leidingen maken aan de hand van een concreet voorbeeld
- ✓ De verantwoordelijkheden van de verschillende partijen (eigenaar van de activa, integrator, productleverancier) vaststellen
- ✓ De norm 62443 in het regelgevingslandschap plaatsen (NIS2, ANSSI-richtlijnen)

Doelgroep

Gemengd publiek uit de IT- en OT-sector: SOC-analisten, CISO's, ingenieurs in industriële systemen, automatiseringsspecialisten, OT-projectleiders, integrators, auditors, cybersecurityconsultants.

Voorafgaande vereisten

Basiskennis van cyberbeveiliging van industriële systemen (PLC, SCADA, sensoren) of cyberbeveiliging van IT-netwerken en -systemen, en cyberbeveiliging (CIA, verdedigingslagen).

Opleidingsprogramma

DEELNEMERS

Gemengd publiek uit de IT- en OT-sector: SOC-analisten, CISO's, ingenieurs in industriële systemen, automatiseringsspecialisten, OT-projectleiders, integrators, auditors, cybersecurityconsultants.

VOORAFGAANDE VEREISTEN

Basiskennis van cyberbeveiliging van industriële systemen (PLC, SCADA, sensoren) of cyberbeveiliging van IT-netwerken en -systemen, en cyberbeveiliging (CIA, verdedigingslagen).

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...

De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

1 industriële cyberbeveiliging

- Fundamentele verschillen tussen IT en OT: prioriteiten (CIA versus AIC), realtime-beperkingen, lange levenscycli, bedrijfszekerheid.
- Overzicht van opvallende incidenten: Stuxnet, Triton/Trisis, Industroyer, Colonial Pipeline.
- Referentiearchitectuur: het Purdue-model (niveaus 0 tot en met 5).

2 Overzicht van de ISO/IEC 62443-normenreeks

- Herkomst van de norm: ISA-99? IEC 62443.
- Indeling in 4 categorieën: algemeen, beleidsregels en procedures, systeem, onderdeel.
- Overzicht van de belangrijkste documenten: 62443-1-1, 2-1, 2-4, 3-2, 3-3, 4-1, 4-2.
- De drie belangrijkste rollen: asset owner, system integrator, product supplier.

Casestudy

Rollenoverzicht — aan de hand van een schema van een fictieve fabriek vaststellen wie wat doet en welk document 62443 op elke actor van toepassing is.

3 De onmisbare woordenschat van de 62443

- IACS, SUC (System Under Consideration), essentiële functie.
- Zones en leidingen: definities, groeperingsprincipes.
- Beveiligingsniveaus: SL-T (doel), SL-A (bereikt), SL-C (capaciteit), SL 1 tot en met 4.
- Bedreigingsactoren volgens 62443: van scriptkiddie tot natiestaat.

4 De 7 fundamentele vereisten (FR)

- FR1: Identificatie- en authenticatiecontrole (IAC).
- FR2: Use Control (UC).
- FR3: Systeemintegriteit (SI).
- FR4: Vertrouwelijkheid van gegevens (DC).
- FR5: Beperkte gegevensstroom (RDF).
- FR6: Tijdige reactie op gebeurtenissen (TRE).
- FR7: Beschikbaarheid van middelen (RA).
- Verband tussen FR, systeemvereisten (SR) en componentvereisten (CR).

Groepsdiscussie

Groepsanalyse van een FR met de bijbehorende SR's en Requirement Enhancements (RE) op basis van de beoogde SL.

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

- De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
- Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
- Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

5 Risicoanalyse volgens 62443-3-2

- Het ZCR-proces (Zone and Conduit Requirements) in 7 stappen.
- Identificatie van het SUC en eerste indeling in zones/leidingen.
- Eerste risicobeoordeling en vaststelling van de SL-T.
- Het begrip aanvaardbaar risico en iteratie.

Casestudy

(In een kleine productiefabriek met MES, SCADA, PLC's, sensoren en externe toegang voor leveranciers) verdelen de deelnemers het systeem op een papieren plattegrond in zones en leidingen, motiveren ze hun keuzes en wijzen ze aan elke zone een SL-T toe.

6 Van de SL-T naar concrete maatregelen

- Hoe zet je het beoogde beveiligingsniveau om in technische en organisatorische vereisten?
- Praktische uitleg van 62443-3-3 (Systeemvereisten).
- Praktische uitleg van de norm 62443-4-2 (Component Requirements) voor producten.
- Consistentie SL-T/SL-C/SL-A: wat te doen als een onderdeel de beoogde SL niet haalt? (compenserende maatregelen)

Casestudy

Geef voor een bepaald gebied een overzicht van de toepasselijke SR's op basis van de gekozen SL-T en breng de verwachte afwijkingen ten opzichte van een typisch bestaand industrieel ontwerp in kaart.

7 Organisatorisch aspect: 62443-2-1 en 2-4

- 62443-2-1: het CSMS (Cyber Security Management System) vanuit het perspectief van de eigenaar van de activa.
- 62443-2-4: eisen voor integratie- en onderhoudsdienstverleners.
- Verband met een bestaand ISO 27001-informatiebeveiligingsbeheersysteem (ISMS): complementariteit, geen redundantie.
- Veiligheidslevenscyclus: ontwerp, integratie, exploitatie, ontmanteling.

8 Productonderdeel: 62443-4-1 en certificering

- 62443-4-1: Secure Development Lifecycle (SDL) aan de kant van de leverancier.
- 62443-4-2: technische vereisten per type component (software, ingebedde systemen, netwerk, host).
- Overzicht van certificeringen: ISASecure, IECEE en hun waarde bij een aanbesteding.
- Regelgevend kader en ecosysteem: de rol van 62443 binnen NIS2 en de REC-richtlijn.
- ANSSI-richtlijnen inzake cyberbeveiliging van industriële systemen en de koppeling daarvan met 62443.
- Aanvullende normen: NIST SP 800-82, IEC 62351.
- Bronnen uit de gemeenschap, ervaringen uit de praktijk, organisaties (ISA, CLUSIF, CESIN).

Casestudy

Een technisch gegevensblad van een industrieel apparaat analyseren en de elementen identificeren die (al dan niet) aantonen dat het voldoet aan de norm 62443-4-2.

Dit programma is een origineel concept, ontwikkeld door de pedagogische teams van ORSYS Formation. Elke reproductie, weergave, aanpassing of exploitatie, geheel of gedeeltelijk, zonder voorafgaande schriftelijke toestemming van ORSYS, is ten strengste verboden. ORSYS behoudt zich het recht voor om alle nodige maatregelen te nemen ter bescherming van haar intellectuele-eigendomsrechten.

Data en plaats

KLAS OP AFSTAND

2026 : 30 nov.

2027 : 15 maa., 14 juni, 9 sep., 6 dec.

PARIS LA DÉFENSE

2027 : 8 maa., 7 juni, 2 sep., 29 nov.