Mondragon Unibertsitatea

ZIBERSEGURTASUN INDUSTRIALEAN ONLINE IKASTAROA

GAIA	Informatika, Telekomunikazio Sistemak eta Sistema Txertatuak
ECTS/ORDUAK	1 ECTS
EGUTEGIA	2027/01/18 - 2027/03/12 As-At-Az-Og-Or
HIZKUNTZA	Gaztelania
MODALITATEA	Online

Informazio gehiago eta izen-ematea

HELBURUAK

Aurrerapen teknologikoek abantaila, onura eta ekarpen ugari ekarri dizkiote enpresa-jarduerari, bai informazioaren teknologietan, bai eragiketetan. Hala ere, abian jartzeak berekin dakar zenbait arriskuri aurre egitea, eta arrisku horiek arindu, murriztu edo transferitu egin beharko dira, erakundeak bere gain har dezakeen puntu bateraino.

Konpainiek aurrekaririk gabeko gardentasuna dute eragiketa guztietan, eta, prozesuak hobetzeaz gain, negozio-eredu berriak ere garatuko dituzte, irabaziak handitzeko.

Produkzio-denborak murriztea, malgutasuna handitzea, masako ekoizpen indibidualizatua ahalbidetzea eta energiaren eta baliabideen kontsumoa optimizatzea dira enpresek gaur egun dituzten erronketako batzuk, eta balio-kate osoa optimizatu behar dute, produkzioaren diseinutik, plangintzatik eta ingeniaritzatik hasi eta zerbitzuetaraino. Erabilgarritasuna handitzea, etengabeko hobekuntza, prozesuen optimizazioa eta erresilientzia, edozein azpiegitura motaren gainean planifikatu gabeko etenduren aurrean, dira helburu nabarmenetako batzuk; adibide argiak aurkitu ditugu manufaktura-industrian, energian, makina-erremintan edo automobilgintzan.

Beraz, eskuragarri dauden datu asko bildu, testuinguruan kokatu eta aztertzean, enpresek informazio eraldatzailea lortuko dute, erabaki informatuak hartzeko eta errentagarritasuna hobetuko duten aldaketak egiteko. Prozesuei edo prozesuei lotutako informazioa sortzeak, eskuratzeak, tratatzeak eta ustiatzeak soluzio berriak abian jartzeko funtsezko alderdi bat errazten du, elkarreragingarritasuna. Horrek, teknologien integrazioarekin batera, sistema, osagai eta gailu horien esposizio-maila handitzen du.

Zibersegurtasun industriala ekintzen, metodoen eta prozeduren multzoa da, teknikoak zein operatiboak, aukera ematen dutenak arrisku-maila hori gutxieneko onargarria izan dadin eta, halaber, erakundearentzat intzidente baten bidezko inpaktua, horiek behar ez bezala erabiliz edo eskuratuz gero, minimoa izan dadin.

Hau da, saihestu egin behar da zerbaitek edo norbaitek, nahita edo nahi gabe, enpresa, erakunde edo erakunde baten jarduera osorik edo zati batean aldatzea, eta, horrela, kalte materiala edo ez-materiala eragitea, sartutako arrisku teknologiko berrien ondorioz, eta mehatxuek eta kalteberatasunek beren helburuak lortzeko bidea aurkitzea.

Horregatik, nahitaez babestu behar dira konpainien negozio-ereduen oinarri diren industria-jarduera eta -prozesuetan esku hartzen duten sistema, gailu eta osagai horiek, bai eta prozesuetako informazioa sortzen, eskuratzen, tratatzen eta biltegiratzen parte hartzen dutenak ere.

NORI ZUZENDUA

Informazio-teknologiekin lotutako langileak, sareen, sistemen edo garatzaileen administratzaile gisa; eta operaziokoak, programatzaile, mantentze-lanetako edo ingeniaritzako langile gisa.

PROGRAMA

1. "Zibersegurtasun industrialerako sarrera" modulua (Iraupena: ordubete)
a. Eragiketa-teknologien definizioa.
b. Industria-iraultzen bilakaera.
c. Iraganeko eta egungo egoera.
d. Aldeak eta lehentasunak IT eta LB inguruneetan.
e. Zibersegurtasun industrialaren onurak.
f. Gertakarien adibideak.

2. "Ekipo eta gailu industrialak" modulua (Iraupena: 2h 20m)
a. Sentsoreak, eragingailuak.
b. PLCak eta kontrolagailuak.
c. Segurtasun Funtzionala, SIS.
d. Periferia deszentralizatua.
e. HMI, bistaratze-sistemak.
f. Programazio-softwarea.
g. Robotak.
h. DCS.
i. VFD.
j. Networking industriala.
k. Pasabideak.
l. SCADA, MES eta ERP zerbitzariak.
m. Makina-erreminta.
n. 1. jarduera: "Ekipamendu eta gailu nagusiak identifikatzea eta proposatutako eszenatoki batean kokatzea".

3. "Industria-sareak eta -komunikazioak" modulua (Iraupena: 1h 43m)
a. Komunikazioetarako sarrera.
b. OSI erreferentzia-eredua.
c. TCP/IP pila.
d. Tresneriaren identifikatzaileak.
e. VLAN
f. Industria-komunikazioen motak eta ezaugarriak.
g. Betekizunak.
h. Industria-komunikazioen ereduak.
i. Gailuak.
j. Protokoloak eta eremu-busak.
k. Sare industrialen topologiak.

l. Baliabide fisikoak eta hari gabekoak.
m. Komunikazioen bilakaera.
n. 1. jarduera: "Trafikoaren analisia, harrapaketetatik abiatuta"

4. "Purdue eredua eta ISA- 95" modulua (Iraupena: 10 m)
a. Sarrera.
b. Eredua geruzaka.
c. Geruzen definizioa.
d. Prozesu motak.
e. 1. jarduera: "1. jarduerako ekipoak eta gailuak kokatzea, Purdue modeloaren arabera"

5. "Mehatxuak industria-inguruneetan" modulua (Iraupena: 24m)
a. Mehatxuen definizioa.
b. Nahita egindakoak.
c. Nahi gabekoak.
d. Barnekoak.
e. Kanpokoak.
f. Sartzeko bidea.
g. Arrisku-faktoreak.

6. "Industria-inguruneetako kalteberatasunak" modulua (Iraupena: 36m)
a. Definizioa.
b. Sailkapena eta kategorizazioa.
c. Kalteberatasunen presentzia industria-inguruneetan.

7. "Industria-inguruneetako eraso-bektoreak" modulua (Iraupena: 20 m)
a. Definizioa.
b. Erabilitako mekanismoak eta metodoak.

8. "Defentsa Sakoneko Eredua" modulua (Iraupena: 2h 5m)
a. Definizioa.
b. Security eta Safety desberdintasunak.
c. Industria-inguruneek babesteko dituzten erronkak.
d. IT eta OT defentsa-estrategiaren arteko aldea.
e. Babes-metodoak eta -baliabideak.
f. Geruzakako eredua eta haren esanahia.
g. Horietako bakoitzaren azalpena.
h. Mugak.
i. Defentsa Ereduan esku hartzen duten osagaiak eta elementuak
Sakonera.
j. Inplementazio-eredua.

9. "Komunikazio-azpiegiturei buruzko segurtasun-neurriak" modulua
(Iraupena: 2 h 25 m)
a. Definizioa.
b. Helburuak.
c. Inguruneak.
d. NGFW.
e. Zonak.
f. Bereizketa.

g. Segmentazioa.
h. Mikro segmentazioa.
i. Virtual Patching.
j. VPNak.
k. Monitorizazioa.
l. Beste gogoeta batzuk.
m. Lotutako zereginak.
n. 1. jarduera: "Galderei erantzutea eta suebaki-ekipoak" Erreferentzia-ereduak "moduluaren 1. jardueraren eskeman kokatzea.
o. Demo 1; "Trafiko-harrapaketa", Port Mirror eta TAP.
p. Demo 2; "Sareko suebakiak, I. zatia"; funtzionaltasunak eta adibideak Fortinet Fortigate eta SIEMENS Scalance S eta X ekipoekin.
q. Demo 3; "Sareko suebakiak, II. zatia; NGFW, eragiketa moduak, DPI, etab. Fortinet Fortigate eta SIEMENS Scalance S eta X. ekipoekin egindako adibideak"

10. "Azken ekipoetako segurtasun-neurriak" modulua (Iraupena: 1h 37m)
a. Definizioa.
b. Bastioitzea.
c. Whitelisting.
d. Sarbideen kontrola.
e. Monitorizazioa.
f. Biruskontrakoak.
g. Adabakien kudeaketa.
h. Zifratzea.
i. Aktiboen kudeaketa.
j. Babes-kopiak.
k. Urruneko sarbidea.
l. Sistema

IRAKASLEAK

Echave Garcia, Edorta

EGUTEGIA

2027/01/18 - 2027/03/12

Astelehena-Asteartea-Asteazkena-Osteguna-Ostirala

00:00-23:59
