Mondragon Unibertsitatea

# MONITORIZAZIOA ETA ZIBERGORABEHEREI ERANTZUTEA UNIBERTSITATE MIKRO-KREDENTZIALA (ONLINE)

| | |
|---|---|
| GAIA | Informatika, Telekomunikazio Sistemak eta Sistema Txertatuak |
| ECTS/ORDUAK | 3.5 ECTS |
| EGUTEGIA | 2026/09/07 - 2026/11/06 |
| HIZKUNTZA | Gaztelania |
| MODALITATEA | Online |

**Informazio gehiago eta izen-ematea**

## HELBURUAK

- Segurtasun-eragiketen zentro (KSA) baten barruan monitorizazioaren, detekzioaren eta erantzunaren zeregina ulertzea.
- Defentsa sakoneko estrategia aurreratuak eta Zero Trust aztertzea eta inplementatzea.
- Monitorizazio-metodologiak aplikatzea SIEMekin, threat hunting-ekin, gorabeherei emandako erantzunarekin eta auzitegiko analisiekin.
- Wazuh, Prometheus, Autopsy, Volatility, EDR, SOAR, Nessus eta OpenVAS bezalako tresnak erabiltzea.
- DevSecOps-en arriskuen kudeaketa (GRC) eta praktikak integratzea erakundearen defentsan.
- Zibersegurtasunean adimena eta kontrainteligentzia ikertzeko gaitasunak garatzea.

## PROGRAMA

- **Defentsa-segurtasun aurreraturako sarrera.** Modulu honek defentsa-segurtasunaren funtsezko printzipioak jorratzen ditu, eta defentsa sakonak eta segurtasun-geruza anitzen koordinazioak duten

garrantzia nabarmentzen du. KSA batean funtsezko rolak aztertzen dira, hala nola gertaeren analisia, eta segurtasun-arrakalen azterketa-kasuak berrikusten dira. Arriskuen kudeaketa eta GRC esparrua ere sartzen dira, arriskuak identifikatzeko, ebaluatzeko eta kontrolatzeko estrategiak aplikatzeko ariketa praktikoekin.

- **Kontzientziazioa.** Erakundeen barruan informazioaren segurtasunari buruzko kontzientziazio-kultura bat sortzera bideratuta dago. Zibersegurtasunari buruzko prestakuntza- eta sentsibilizazio-programa eraginkorrak ezartzeko adibideak eta baliabideak ematen ditu.

- **Gorabeherak monitorizatzea eta detektatzea.** Modulu honek sareetako segurtasun aurreratua aztertzen du, segmentazio eta Zero Trust kontzeptuak barne, baita gertaerak monitorizatzeko SIEMen erabilera ere. Wazuh eta Prometheus tresnekin ariketa praktikoak egiten dira, ingurune korporatiboetan anomaliak detektatzeko eta alertak sortzeko.

- **Threat Hunting eta Gertaerei Erantzutea.** Threat hunting teknika aurreratuak aurkezten ditu, mehatxu-adimenaren erabilera eta konpromiso-adierazleak barne. Gainera, gorabeherei erantzuteko prozesua zehazten da, detekziotik berreskurapenera bitarteko simulazio praktikoekin, EDR eta SOAR bezalako tresnak erabiliz.

- **Auzitegiko analisia eta datuak berreskuratzea.** Modulu honek auzitegiko informatikari buruzko sarrera zehatza eskaintzen du, memoria eta artefaktu digitalak aztertzeko Autopsy eta Volatility tresnen erabilera barne. Ebidentziak babesteko eta auzitegi-txostenak sortzeko teknika aurreratuak estaltzen dira, aurkikuntzak jakinarazteko.

- **Azpiegituren ebaluazioa eta defentsa.** Nessus eta OpenVAS bezalako tresnen bidezko kalteberatasunen ebaluazioan oinarritzen da, baita defentsa perimetralen inplementazioan ere, firewall-ak eta WAFak barne. Ariketa praktikoak egiten dira defentsa horien eraginkortasuna simulatutako inguruneetan konfiguratu eta probatzeko.

- **Inteligentzia eta Kontrainteligentzia Ikerketa.** Aztertu mehatxuak identifikatzeko inteligentzia biltzeko eta aztertzeko teknika aurreratuak. Gainera, emaitzak modu argi eta eraginkorrean dokumentatzeko eta aurkezteko metodologiak nabarmentzen dira.

- Softwarearen garapenaren bizi-zikloan segurtasun-praktikak integratzeari heltzen dio. DevOps inguruneetako segurtasuna automatizatzeko tresna eta teknika espezifikoak arakatzen dira, hornidura-katean eta garapen-prozesu osoan babesa bermatuz.

Bloke honetako jarduera praktikoetan sartzen dira Segurtasun Eragiketen Zentro (KSA) batetik

monitorizatzeko zerbitzuak hedatzeko ariketak, azpiegituretako segurtasun-azterketak, threat hunting ariketa bat ingurune simulatu batean, eta segurtasun-ebaluazio bat GRC framework baten bidez.

## IRAKASLEAK

Beleña De Lamor, Joel

---

https://www.mondragon.edu/cursos/eu/ikastaroa/monitorizazioa-eta-zibergorabeherei-erantzutea