Mondragon Unibertsitatea

Formación para Profesionales

Ikastaroa Incidentes de Seguridad (online)

Gaia Informatika, Telekomunizio Sistemak eta Sistema Txertatuak

ECTS/orduak 100 ORDU

Egutegia 2017/05/01 - 2017/05/21 As-At-Az-Og-Or

Ordutegia 08:00-18:00

Hizkuntzak Gaztelania

Modalitatea Online

Prezioa 625 €

Helburuak

" Poder desarrollar políticas de seguridad que permitan una mejor gestión de la seguridad informática dentro de la organización.
" Estudiar los riesgos que soporta un Sistema de Información y el entorno asociado con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio.
" Conocer las medidas apropiadas que deberían adoptarse para prevenir, impedir, reducir o controlar los riesgos de seguridad informática.
" Ser capaz de implantar con éxito mecanismos de seguirdad.
" Ser capaz de evaluar el nivel de seguridad de la organización e identificar los aspecto a mejorar.

Nori zuzendua

Responsables de Seguridad Informática.
Administradores de Redes y Sistemas.
Técnicos informáticos.

Egitaraua

- Gestión de Incidentes
    - Equipos de respuesta a incidentes
        - CERT

- Procedimiento de respuesta a incidentes
    - Preparación
    - Detección y Análisis
    - Eliminación y Recuperación del incidente
    - Post-Incidente: Informe de incidentes
- Herramientas
    - RTIR: Request Tracker for Incident Response
    - OTRS: Open Ticket Request System
- Detección de intrusiones
    - Definiciones
    - Historia de los IDS
    - Clasificación
        - Fuentes de Información
- Host Based Intrusion Detection (HIDS)
- Network Based Intrusion Detection (NIDS)
- Métodos de Análisis

- Detección en Anomalías
- Tiempo
- IDS en Tiempo Real
- IDS en Batch
- Respuesta
- Pasiva
- Activa (IPS)
- Correlación de Eventos
- Herramientas
- Snort NIDS
- OSSEC
- Samhain
- Prelude/OSSIM
- Sistemas trampa: honeypots y honeynets

    - Definiciones
    - Ventajas e Inconvenientes
    - Clasificación de los Sistemas Trampa
        - Según su objetivo
        - Según su nivel de interacción
    - Arquitectura de los sistemas trampa
        - Sistemas trampa físicos
        - Sistemas trampa virtuales
        - Captura de datos
    - Honeynets o redes trampa
    - HoneyClients

- Análisis forense

    - Definiciones

    - Informática Forense: El principio de intercambio de Locard
    - Evidencia Digital
    - Escena del Crimen
  - Pasos ante un Incidente
    - Pre-incidente
    - Detección del Incidente
    - Investigación (Metodologías)

- La Escena del Crimen
- Recogida de Evidencias
- Interpretación de las Evidencias
- Elaboración de la Hipótesis e Informe Final

  - Legislación
    - Acciones post-forense
  - Herramientas
    - Para la Recolección de Evidencias
    - Para Análisis Forense
    - Live CDs

Irakasleak

Fernández Arrieta, Miguel
Lizarraga, Jesús
Lizarralde, Miren Osane
Perez Reguera, Itziar
Uribeetxeberria Ezpeleta, Roberto
Velez De Mendizabal, Iñaki
Zurutuza Ortega, Urko

---

https://www.mondragon.edu/cursos/es/tematicas/informatica-telecomunicaciones-sistemas-empotrados/curso/incidentes-de-seguridad-online