

# RESPONDING TO CYBERSECURITY INCIDENTS USING THREAT INTELLIGENCE

Trainer: [Roberto Martínez](#)

## Descripción general:

En este training el participante aprenderá a aplicar las mejores prácticas en respuesta a incidentes para detectar, contener y recuperarse de ciberataques utilizando cacería e inteligencia de amenazas. También aprenderá a utilizar diferentes herramientas, así como a implementar y orquestar diferentes plataformas de respuesta a incidentes, monitoreo, inteligencia e investigación

## Nivel del curso:

Básico – Intermedio – Avanzado (se van revisando temas a diferente nivel durante el desarrollo del entrenamiento)

## Dirigido a:

Dirigido a profesionales de seguridad o cualquier persona que quiera aprender acerca de gestión de incidentes, procedimientos de primera respuesta, cacería de amenazas y de inteligencia de amenazas utilizando una variedad de plataformas y herramientas.

## Requisitos (conocimientos o de máquina si es necesario) :

Conocimientos básicos de Linux, Windows internals y protocolos de red.

Los ejercicios se realizan sobre equipos virtuales en la nube, por lo que se puede utilizar cualquier equipo corriendo sobre Windows, Linux y Mac.

El participante recibirá de cortesía el libro [“Incident Response with Threat Intelligence”](#) como parte del material del curso

## Temario:

- 1 - Basics of the Incident Response and Triage Procedures
- 2 - Using Cyber Threat Intelligence in Incident Response
- 3 - Creating Incident Response Plans and Playbooks
- 4 - Implementing an Incident Management System
- 5 - Integrating SOAR Capabilities into Incident Response
- 6 - Working with Analytics and Detection Engineering in Incident Response
- 7 - Creating and Deploying Detection Rules
- 8 - Hunting and Investigating Security Incidents

Reservá tu lugar


Costo:

USD 1.500

ARS 438.000

Reservá tu lugar

CONSULTAS

Para realizar consultas sobre el training o alguno de sus beneficios, escribir a: [capacitacion@ekoparty.org](mailto:capacitacion@ekoparty.org)

Trainer:

Roberto Martínez



Security Researcher & Threat Intelligence Analyst.

Digital Forensics Investigator, Incident Responder, and Threat Hunter.

Former Security Consultant and Trainer for Governments, Military, Intelligence Agencies, Financial Institutions and Private Corporations in Latin America.

Member of the High Technology Crime Investigation Association (HTCIA).

Author of the book ["Incident Response with Threat Intelligence"](#)

## Resources

- [ARCHIVE: PAST EDITIONS](#)
- [CODE OF CONDUCT](#)
- [NEWSLETTER](#)
- [EKOMAGAZINE](#)

## About Ekoparty

- [OVERVIEW](#)
- [CTFs & CHALLENGES](#)
- [HACKTIVITIES](#)
- [SPONSORS](#)

✉ [organizacion@ekoparty.org](mailto:organizacion@ekoparty.org)

Copyright

ekoparty security conference

English ▲