FICHA DE TALLER

➢ Datos generales:

Título:	**Monitoreo de Seguridad en Tiempo Real con Herramientas Open Source**					
Instructor o docente:	Rafael Arellano Nava					
Duración total de taller:	4 sesiones virtuales de 2 hrs. C/U, 1 sesión presencial de 3 horas					
Área:	☐	Formación para la docencia	☐	Formación para la gestión universitaria	☐	Otra
Modalidad de impartición:	☐	Presencial	☐	A distancia	☒	Híbrida
Fechas:	2, 9, 16, 23 y 29 de octubre					

➢ Descripción:

Destinatarios:
A aquellos SysAdmin o especialistas en seguridad que requieran herramientas óptimas de bajo costo

Objetivo(s) o competencia(s):
Aprender a instalar herramientas opensource de seguridad como análisis de vulnerabilidades, detectores de intrusos, colectores de datos para orquestarlos y/o administrarlos de manera efectiva

Metodología y Actividades:
Aprender la teoría del monitoreo enfocado a seguridad en tiempo real

Mecanismo y criterios de evaluación:
Asistencia y realización de actividades

- **Temario:**

No. De sesión	Fecha	Hora	Temas a abordar
Sesión 1	2 de octubre	12:00 – 14:00 hrs	Teoría e introducción del monitoreo de seguridad
Sesión 2	9 de octubre	12:00 – 14:00 hrs	Herramientas de monitoreo Open Source tradicionales
Sesión 3	16 de octubre	12:00 – 14:00 hrs	Herramientas OpenSource SIEM
Sesión 4	23 de octubre	12:00 – 14:00 hrs	Instalación y uso de Prelude Wazuh
Sesión 5	29 de octubre	16:00 – 19:00 hrs	Análisis y monitoreo

- **Bibliografía**

8 Open Source SIEM Tools You should know

https://www.lumificyber.com/blog/8-open-source-siem-tools-you-should-know/#:~:text=Deploying%20an%20open%20source%20SIEM,that%20competes%20with%20enterprise%20alternatives.

WAzuh Open Source SIEM Tutorial

https://www.youtube.com/watch?v=u4tMvUCUXqY

Open Source SIEM Solutions: A Complete Guide

https://www.linkedin.com/pulse/open-source-siem-solutions-complete-guide-work-sent-zrdrc

- **Recursos y materiales requeridos**

Software para generar 2 máquinas virtuales a nivel local