



Alonso Eduardo
Caballero Quezada
(ReYDeS)

Curso SIEM / XDR con Wazuh 2026

2
Sesiones

6
Horas

En vivo,
Virtual, o
Personalizado



Alonso Eduardo Caballero Quezada

Tengo más de veintidós años de experiencia, y desde hace dieciocho años realizo capacitaciones y consultorías en Hacking, Forense, OSINT, CiberSeguridad, y GNU/Linux

Redes Sociales

[LinkedIn](#)

[X \(Twitter\)](#)

[YouTube](#)

[Facebook](#)

[Sitio Web](#)

[e-mail](#)

[WhatsApp](#)

Presentación

En el escenario actual de ciberseguridad, la dispersión de logs y la ausencia de visibilidad en tiempo real, son los mayores y principales obstáculos para defender la infraestructura de una organización. Para enfrentar amenazas cada vez más complejas, las empresas no únicamente necesitan recolectar eventos, sino centralizar, correlacionar, y responder de maneras automatizada cualquier incidente.

Este curso está diseñado para enseñar a los administradores de sistemas, ingenieros de red, profesionales de TI, y cualquier persona interesada, a desplegar y operar una plataforma de ciberdefensa de nivel empresarial utilizando software libre.

Durante el transcurso de las sesiones se aprenderá a instalar y configurar el entorno Wazuh (All-In-One), conectando agentes en sistemas operativos Windows y GNU/Linux. Se explorarán los módulos defensivos más solicitados por la industria: vigilancia para la integridad de archivos en tiempo real (FIM), auditoría de configuración de seguridad, evaluación de cumplimiento normativo (PCI-DSS, NIST), además de detección automática de vulnerabilidades y software desactualizado en la red.

Además se profundizará en el motor de análisis para crear reglas personalizadas y decodificadores en XML, permitiendo adaptar la plataforma a la realidad operativa de la organización, y así reducir eficazmente los falsos positivos. Finalmente se implementará la funcionalidad de Respuesta Activa (Active Response), automatizando el bloqueo de ataques por fuerza bruta en los firewalls locales, además de garantizar una contención inmediata ante intrusiones.

Al finalizar se tendrá la capacidad técnica necesaria para implementar un Centro de Operaciones de Seguridad (SOC) Open Source, elevando radicalmente la postura defensiva de una infraestructura, sin depender de licencias costosas o comerciales.



Temario

- ¿Porqué necesitamos un SIEM / XDR?
- Introducción a Wazuh
- Arquitectura General de Wazuh
- Modalidades de Despliegue
- Prerrequisitos de Red e Infraestructura
- Despliegue de Wazuh Server (AIO)
- Máquina Virtual
- Primer Acceso al Dashboard
- ¿Cómo funcionan los Agentes Wazuh?
- Registro con Agente vs. Syslog sin Agente
- Despliegue de Agente en Ubuntu Linux
- Despliegue de Agente en Windows (PowerShell)
- Validación en el Dashboard
- Configuración Centralizada de Agentes (agent.conf)
- Monitoreo de Integridad de Archivos (FIM / Syscheck)
- Configuración de FIM
- Simulación de Evento FIM
- Detector de Vulnerabilidades (Vulnerability Detector)
- Activación del Escaneo de Vulnerabilidades
- Marcos de Cumplimiento Normativo (Compliance)
- Evaluación de Configuración de Seguridad (SCA)
- Anatomía del Pipeline de Logs en Wazuh
- Estructura de Niveles de Severidad en Wazuh
- Reglas Base vs. Reglas Locales
- Sintaxis Fundamental de XML en Reglas
- Análisis de Log Crudo (SSH / RDP)
- Creación de Regla Personalizada (local_rules.xml)
- Prueba y Validación de la Regla
- Reducción de Falsos Positivos (Tuneo)
- Concepto de Respuesta Activa (Active Response)
- Componentes de Active Response
- Configuración de Bloqueo Automático por Fuerza Bruta
- Simulación del Ataque de Fuerza Bruta
- Integraciones y Notificaciones Externa
- Buenas Prácticas de Mantenimiento de Wazuh

Beneficios

- Acceso al aula virtual por sesenta (60) días
- Acceso a las sesiones en vivo
- Videos de las dos (2) sesiones
- Acceso libre a las sesiones en vivo de los siguientes cursos a dictarse
- Material utilizado durante el desarrollo del curso
- Asesoría personalizada y permanente
- Certificado digital de participación
- Certificado digital de aprobación por una duración total de 16 horas

Inversión

Perú: S/. 225 Soles

- Depósito o transferencia interbancaria a Scotiabank
- Pago mediante YAPE o PLIN

Otros países: \$ 75 Dólares

- Pago mediante PayPal

Escriba un mensaje al WhatsApp
<https://wa.me/reydes> para proporcionarle los datos pertinentes.

Información

Para obtener más información sobre este curso tiene a su disposición los siguientes mecanismos de contacto.

WhatsApp: <https://wa.me/reydes>

Correo electrónico: reydes@gmail.com