2025

Construcción de un entorno SOC con Wazuh sobre Rocky Linux: guía técnica y experiencia personal

"Compartir conocimiento es construir comunidad. Este proyecto es una invitación a seguir aprendiendo, experimentando y creciendo en este camino tan apasionante que es la ciberseguridad."

Autor: Zahira Marano
AEGIS SEC |

Contenido

Introducción 2
Entorno Tecnológico 2
Implementación paso a paso 2
Recomendaciones 3
Conclusión 3
Recursos útiles 4

Introducción

En un contexto donde la ciberseguridad es cada vez más crítica, decidí montar mi propio entorno SOC (Security Operations Center) para experimentar, aprender y contar con una base sólida para análisis y gestión de incidentes.

Elegí Rocky Linux 9 como sistema base por su estabilidad y compatibilidad con entornos empresariales, pero también podés usar Ubuntu si no tenes conocimientos avanzados en Linux, y Wazuh como plataforma central de monitoreo y correlación de eventos. Esta guía resume tanto el proceso técnico como mi experiencia personal durante la implementación.

Entorno Tecnológico

Sistema operativo: Rocky Linux 9 (mínima instalación)

Herramientas principales:

- ✓ **Wazuh:** SIEM, HIDS y correlación de eventos
- ✓ **Suricata / Zeek**: IDS para análisis de tráfico de red
- ✓ **TheHive:** plataforma de gestión de incidentes
- ✓ **Cortex:** análisis automático de indicadores
- ✓ **MISP** (opcional): inteligencia de amenazas
- ✓ Simuladores: Metasploit, Atomic Red Team, MITRE Caldera

Implementación paso a paso

Preparación del entorno

Instalación de Rocky Linux (mínima)

Configuración de red, hostname, actualizaciones

Ajustes de seguridad (firewall, SELinux en permissive si es necesario)

Instalación de Wazuh

Script oficial desde: https://documentation.wazuh.com/current/installation-guide/

Configuración de Elastic Stack, Filebeat y Wazuh Manager

Acceso al dashboard en https://IP:5601

Agregando endpoints

Instalación de agentes Wazuh en Windows/Linux

Comprobación de logs, alertas y reglas activas

IDS y análisis de tráfico

Instalación de Suricata o Zeek

Redirección de logs a Wazuh para análisis de red

Integración con TheHive y Cortex

Instalación en máquina separada (Ubuntu recomendado)

Configuración de alertas → casos en TheHive

Integración de Cortex para análisis de IoCs desde Wazuh

Simulación de amenazas

Uso de Metasploit, Atomic Red Team o Caldera

Monitoreo de detecciones en tiempo real

Creación de playbooks de respuesta

Backups y optimización

Configuración de retención de logs

Copias de seguridad (manuales o con scripts)

Ajustes de rendimiento para entornos productivos

Recomendaciones

- ✓ Rocky Linux es ideal para producción: sólido, compatible, sin sobresaltos. Pero bastante complejo, si no tenes conocimientos avanzados de Linux te recomiendo usar Ubuntu.
- ✓ La integración entre herramientas requiere paciencia, pero vale la pena: una vez todo está conectado, la visibilidad es excelente.
- ✓ Simular incidentes reales acelera muchísimo el aprendizaje.
- ✓ Documentar cada paso me ayudó a ahorrar tiempo en errores repetidos.

Conclusión

Este proyecto no solo me permitió construir una base técnica sólida, sino que también potenció mi perfil profesional como analista y futura auditora de ciberseguridad.

La experiencia de construir un SOC desde cero con herramientas open source me dio autonomía, visión estratégica y confianza para encarar desafíos reales.

Recursos útiles

- Rocky Linux: https://rockylinux.org/download
- Wazuh: https://wazuh.com
- Suricata: https://suricata.io
- Zeek: https://zeek.org
- TheHive: https://thehive-project.org
- Cortex: https://www.cortex-platform.org
- MISP: https://www.misp-project.org
- Atomic Red Team: https://github.com/redcanaryco/atomic-red-team

- MITRE Caldera: https://github.com/mitre/caldera
- Metasploit: https://docs.rapid7.com/metasploit/
- Repositorios Wazuh: https://github.com/wazuh/wazuh-templates