Alumna: Vispo, Valentina Solange.
Diplomatura Universitaria en Ciberseguridad

wazuh.

Versión 4.7.2

Trabajo Práctico 1

1. ¿Cuál es el propósito general de Wazuh?
    a. *Analizar el tráfico de red de un servidor.*
    b. *Optimizar el rendimiento de un agente.*
    c. *Monitorear y analizar los dispositivos finales como servidores, computadoras de uso personal, etc.*
2. Indique la opción correcta respecto a la arquitectura de Wazuh:
    a. *Se compone de wazuh-manager y wazuh-indexer.*
    b. *Se compone de: wazuh-manager, wazuh-indexer y wazuh-dashboard.*
    c. *Se compone de: wazuh-manager, wazuh-indexer, wazuh-dashboard y wazuh-agent.*
3. El módulo FIM de Wazuh se encarga de:
    a. *Validar el estado de los agentes.*
    b. *Verificar y monitorear la integridad de los archivos de sistema y de aplicaciones.*
    c. *Detectar archivos maliciosos en los dispositivos monitoreados.*
4. ¿Qué capacidad de Wazuh permite automatizar las acciones de respuesta a incidentes de seguridad según desencadenantes específicos?
    a. *Active Response*
    b. *Log Data Collection*
    c. *Monitoring System Calls*
    d. *Vulnerability Detection*
5. ¿En qué consiste el “hardening” o “endurecimiento”, en referencia al módulo SCA?
    a. *Verificar la existencia de archivos, directorios, claves y valores de registro.*
    b. *Reducir la superficie de vulnerabilidad eliminando posibles vectores de ataque.*
    c. *Aumentar la eficiencia computacional de los agentes monitoreados corrigiendo configuraciones incorrectas.*