

Mejoras en IDS: añadiendo funcionalidad a Wazuh

github.com/andresgomezvidal/tfg_memoria

Autor:

Andrés Santiago Gómez Vidal

Directores:

Purificación Cariñena Amigo

Andrés Tarascó Acuña

Introducción

- La seguridad informática avanza continuamente.
- Las medidas de prevención no son suficientes.

Diferencias principales

	IDS	Antivirus tradicional
Recopilación	Información masiva de multiples sistemas	Información local
Análisis	Eventos y flujos de datos	Programas y archivos
Detección	Objetivos	Técnicas

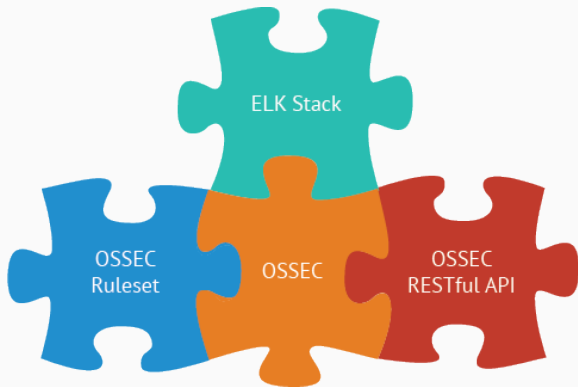
Objetivos

- Detectar posibles intrusiones en sistemas.
- Crear configuración para detectar amenazas reales.

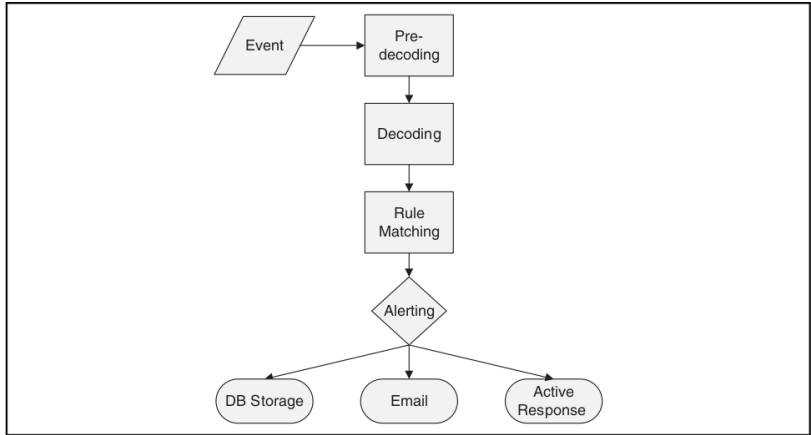
¿Qué es OSSEC?

- Escalable con agentes.
- Basado en reglas y alertas.
- Compatible: Windows, Mac OS, GNU/Linux, etc.
- Integrable: Docker, Puppet, Ansible, OSQuery, VirusTotal, Suricata, OwlH, Bro, etc.

¿Qué es Wazuh?



Procesamiento de reglas



Gestión del proyecto

Tipo de proyecto

- Mezcla entre desarrollo de software e investigación.
- Poco código y simple.

- Alta incertidumbre inicial.
- Fácilmente expandible.

- Generación automática de reglas tomando datos de honeypots.
- IDS con análisis por comportamiento.
- IDS con orientación a tráfico de red.
- Extra análisis del registro de Windows.
- Uso de YARA con Wazuh.
- Generación automática de reglas para Wazuh a partir de Sigma.
- Protección del propio IDS.

- Solamente requisitos no funcionales.

Requisitos esenciales

- ✓ Detección de Golden Tickets.
- ✓ Detección de volcado de memoria de LSASS.
- ✓ Detección de ataque con fuerza bruta inversa.
- ✓ Detección de ataque con fuerza bruta distribuido.
- ✓ Detección de logins fuera de hora.
- ✓ Detección de cryptolockers.
- ✓ Uso de Sysmon para obtener información.

Requisitos deseados

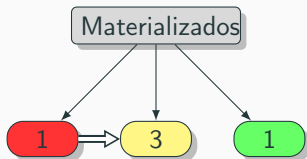
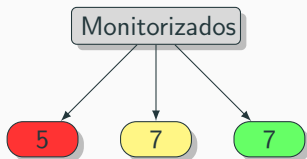
- ✓ Monitorización de archivos trampa.
- ✗ Detección de puertas traseras.
- ✗ Creación de perfiles de configuración.
- ✗ Uso de honeypots con Wazuh.
- ✗ Exploración de soluciones con GPDR.
- ✗ Monitorización de archivos clave en GNU/Linux.

- ✓ Integración de Wazuh con otros programas.

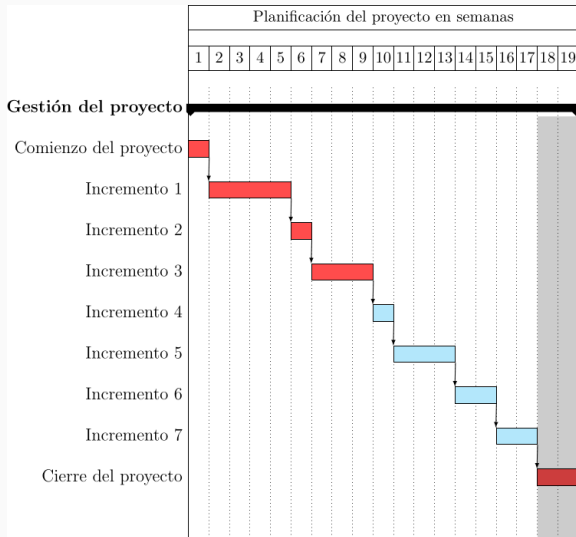
- Poco contacto con el cliente.
- Repartición de requisitos.
- Facilidad de adaptación del alcance.
- Simplicidad.

- ✓ 1: Detección de ataques comunes en Windows Server.
- ✓ 2: Uso de fuentes de datos adicionales.
- ✓ 3: Detección/acción contra ransomware.

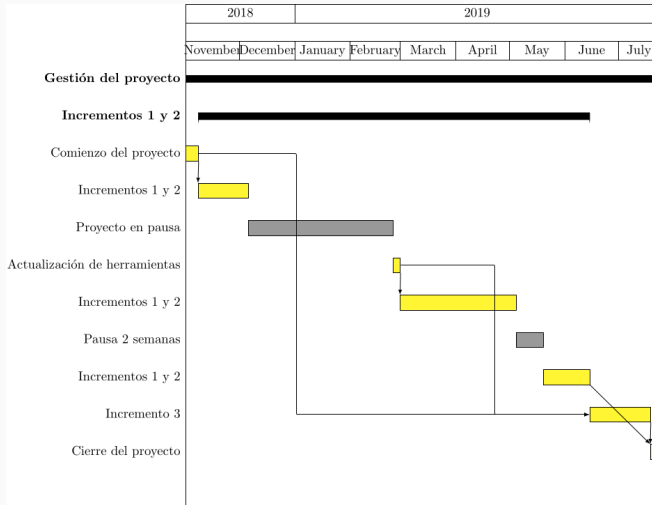
- X 4: Perfiles de configuración para empresas.
- X 5: Exploración de soluciones con GPDR.
- X 6: Detección adicional en GNU/Linux.
- X 7: Integración con VirusTotal.

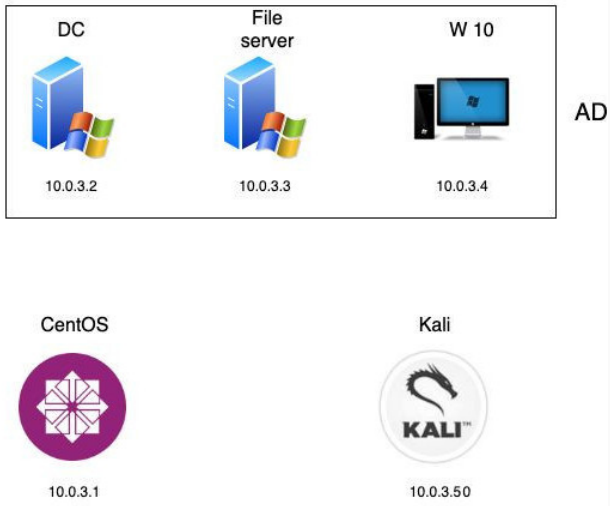


Planificación inicial



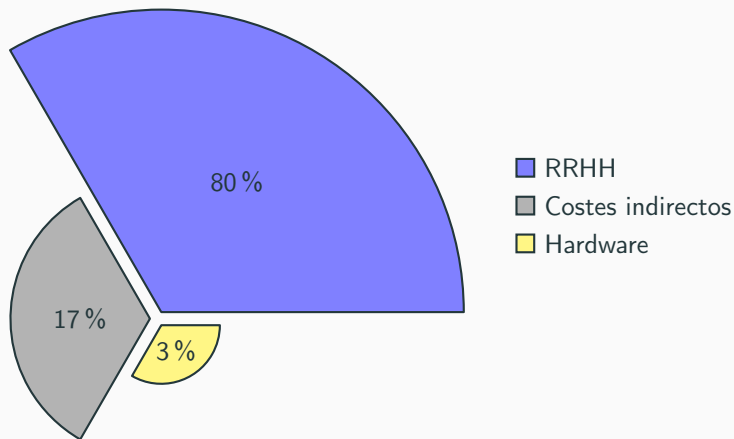
Planificación real





- Identificación y control de los elementos de configuración.
- Git: Código y documentación.
- Backups locales: Máquinas virtuales.

Estimación de costes



$$4897.97\text{€} + 162.39\text{€} + 1012.07\text{€} = 6072.43\text{€}$$

Estimación de costes: RRHH

Papel	Horas	Coste/Hora	Coste total
Jefe de proyecto	22.5	26.78€	602.55€
Ingeniero senior en ciberseguridad	11.25	17.53€	197.21€
Administrador de sistemas	11.25	14.28€	160.65€
Desarrollador junior	418	9.42€	3937.56€

Modelo de trabajo

1. Análisis del ataque.
2. Automatización.
3. Detección.

Tecnologías y herramientas



Sysmon







L^AT_EX



GNU Aspell

Incrementos 1 y 2

- TGT normal \rightarrow Indetectable.
- Ticket válido hasta:
 - Cambio de contraseña de KRBTGT.
 - Expiración del ticket.

- Programas usados.

- Técnicas.
- DLLs.
- Patrones de texto.

- Uso del ticket.

- Usuario raro.
- Longevidad.

- Acceso a archivos clave.
- Volcado de memoria.

- Ejecución codificada.
- PowerShell sin *powershell.exe*.
 - Ejecución encriptada.

- Fuerza bruta.
- Fuerza bruta distribuida.
- Fuera de horas normales.

Incremento 3: Ransomware

- Recurso como rehén.
- Pago anónimo.
- Mercado negro.
- Popularidad reciente.

- Detección lo antes posible.
 - Encriptación masiva de archivos.
 - Borrado de backups.
- Respuesta activa.
 - Matarlo.
 - Apagar.
 - Desconectar de la red.
 - Bloquear acceso a los archivos.
- Dharma.

Conclusiones y trabajo futuro

- Cumplidos los requisitos esenciales, con mucho detalle.
- Tanto IDSs como antivirus tienen sus ventajas y desventajas.
- Mejor estado de GNU/Linux que Windows para Wazuh.

- Mejoras a Wazuh/OSSEC:
 - Creación de reglas.
 - BDD temporal.
 - Active response.
- Incrementos no realizados.
- Límites alcance.

Mejoras en IDS: añadiendo funcionalidad a Wazuh

github.com/andresgomezvidal/tfg_memoria

Autor:

Andrés Santiago Gómez Vidal

Directores:

Purificación Cariñena Amigo

Andrés Tarascó Acuña