Mejoras en IDS: añadiendo funcionalidad a Wazuh

github.com/andresgomezvidal/tfg_memoria

Autor:
Andrés Santiago Gómez Vidal

Tutores:
Purificación Cariñena Amigo
Andrés Tarascó Acuña

Introducción

Motivación

- 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

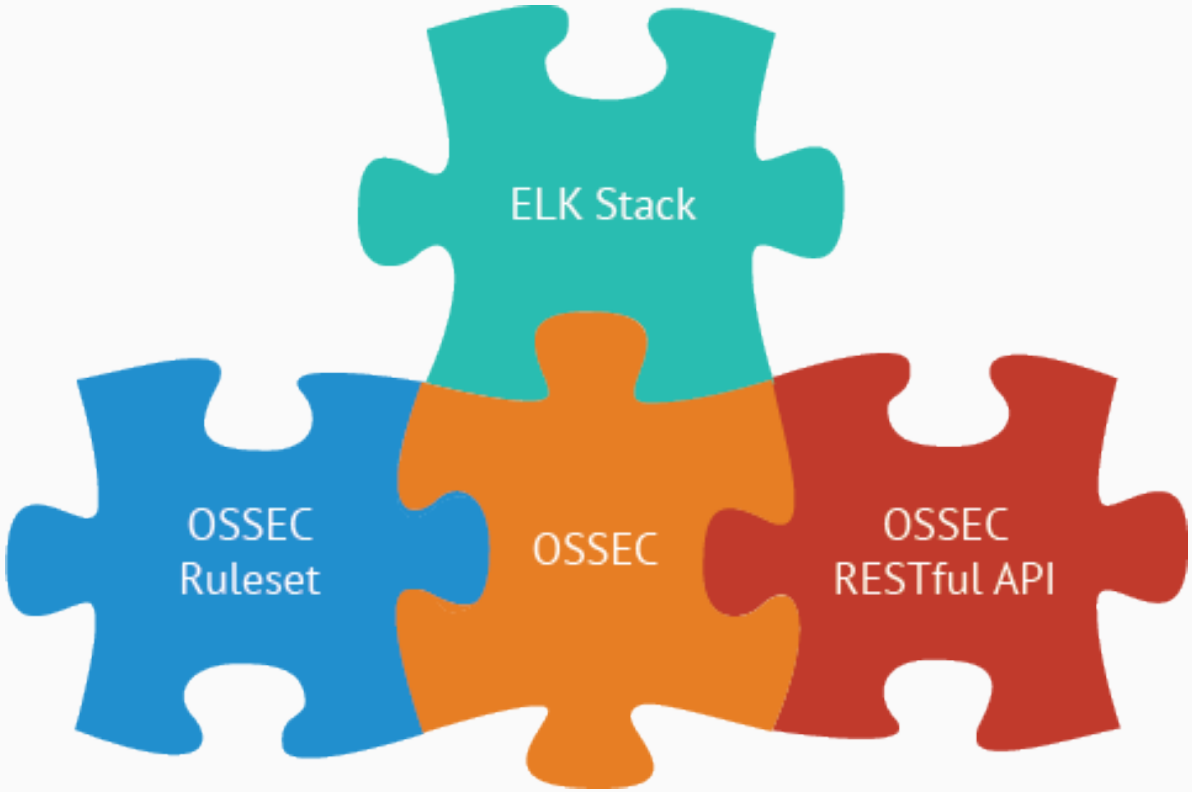
Objetivos

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

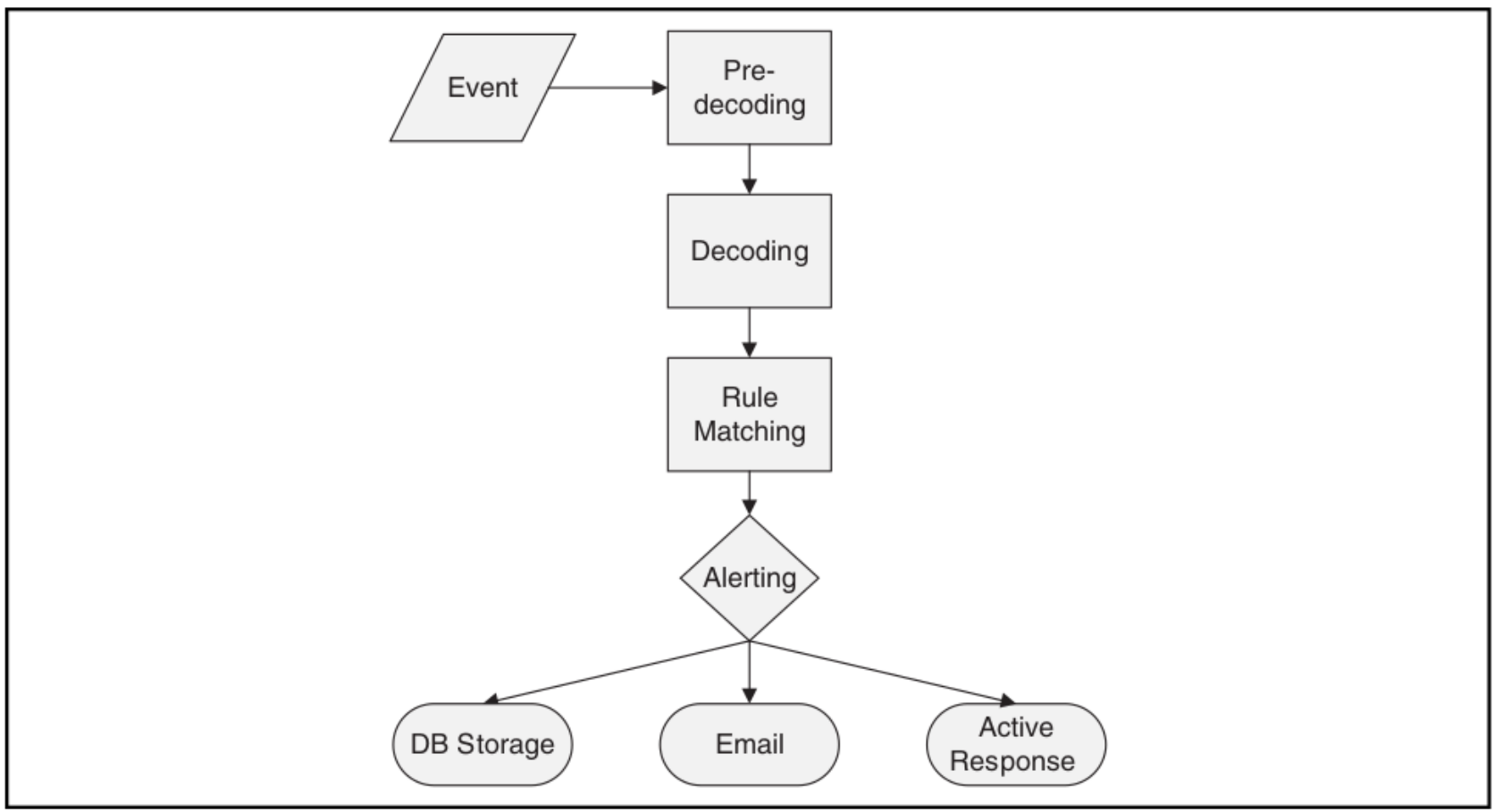
¿Qué es OSSEC?

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

¿Qué es Wazuh?



Procesamiento de reglas



Procesamiento de reglas

- Atómicas y compuestas.
- Estructura padre-hijo.
- Expresiones regulares y variables.
- Pueden no generar ninguna alerta.

Gestión del proyecto

Tipo de proyecto

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

Alcance

- Alta incertidumbre inicial.
- Fácilmente expandible.

Alcance: exclusiones

- Generación automática de reglas tomando datos de honeypots.
- IDS con análisis por comportamiento.
- IDS con orientación a 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.

Requisitos

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

Requisitos opcionales

- ✓ Integración de Wazuh con otros programas.

Metodología: Incrementos

- Repartición de requisitos.
- Facilidad de adaptación del alcance.
- Simplicidad.

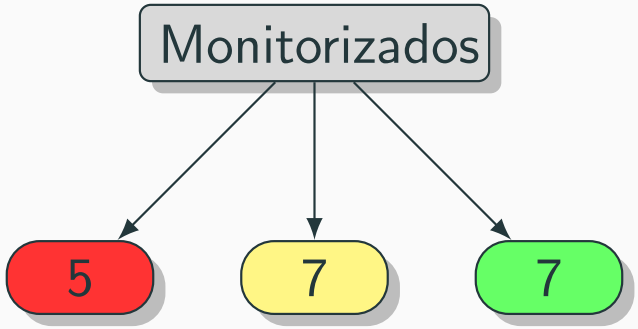
Incrementos esenciales

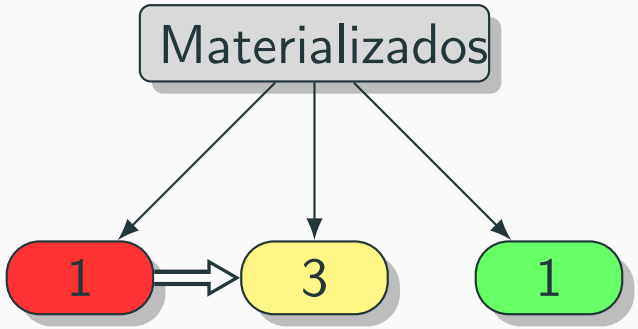
- ✓ 1: Detección de ataques comunes en Windows Server.
- ✓ 2: Uso de fuentes de datos adicionales.
- ✓ 3: Detección/acción contra ransomware.

Incrementos adicionales

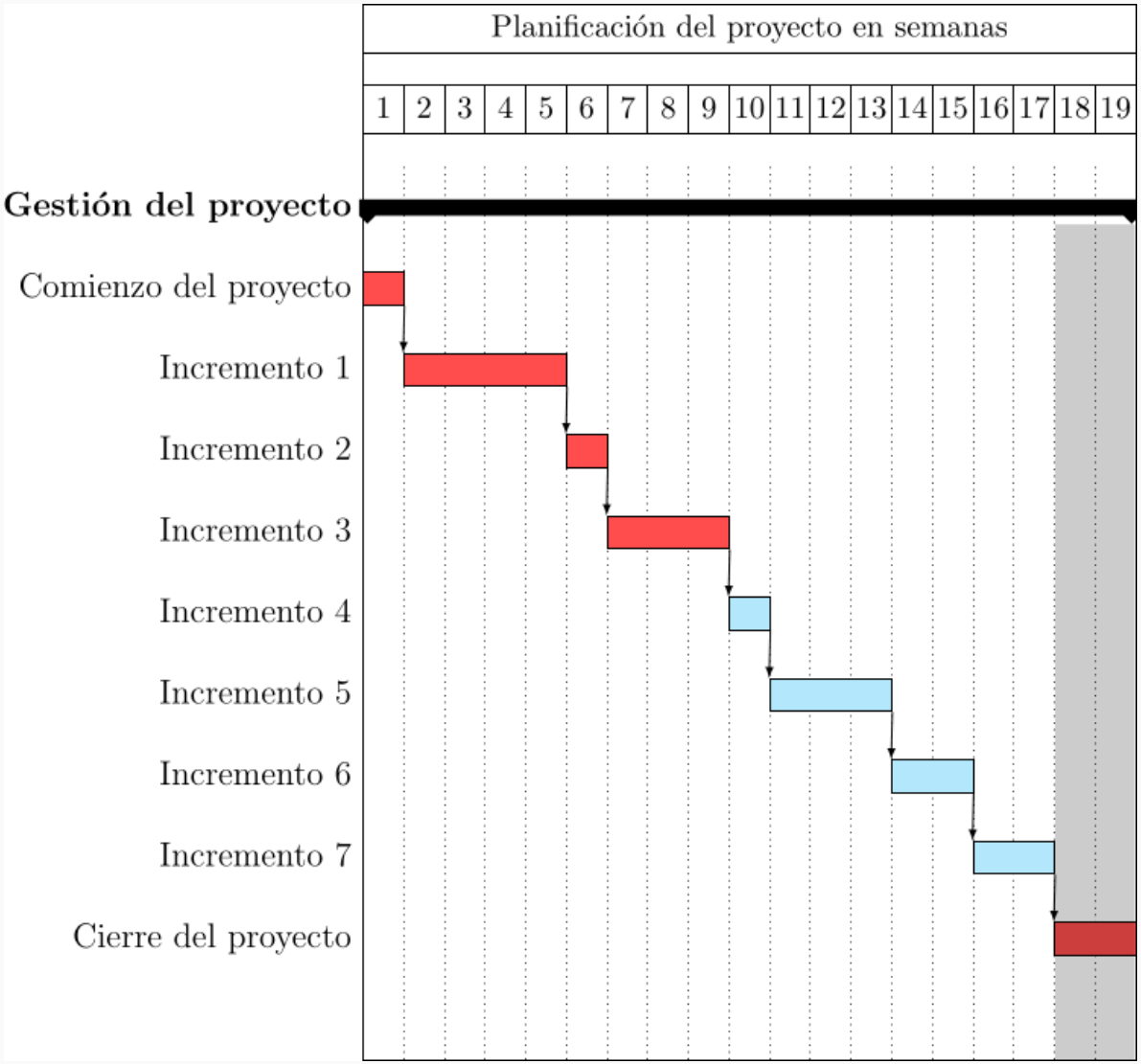
- X 4: Perfiles de configuración para empresas.
- X 5: Exploración de soluciones con GPDR.
- X 6: Detección adicional en GNU/Linux.
- X 7: Integración con VirusTotal.

Riesgos

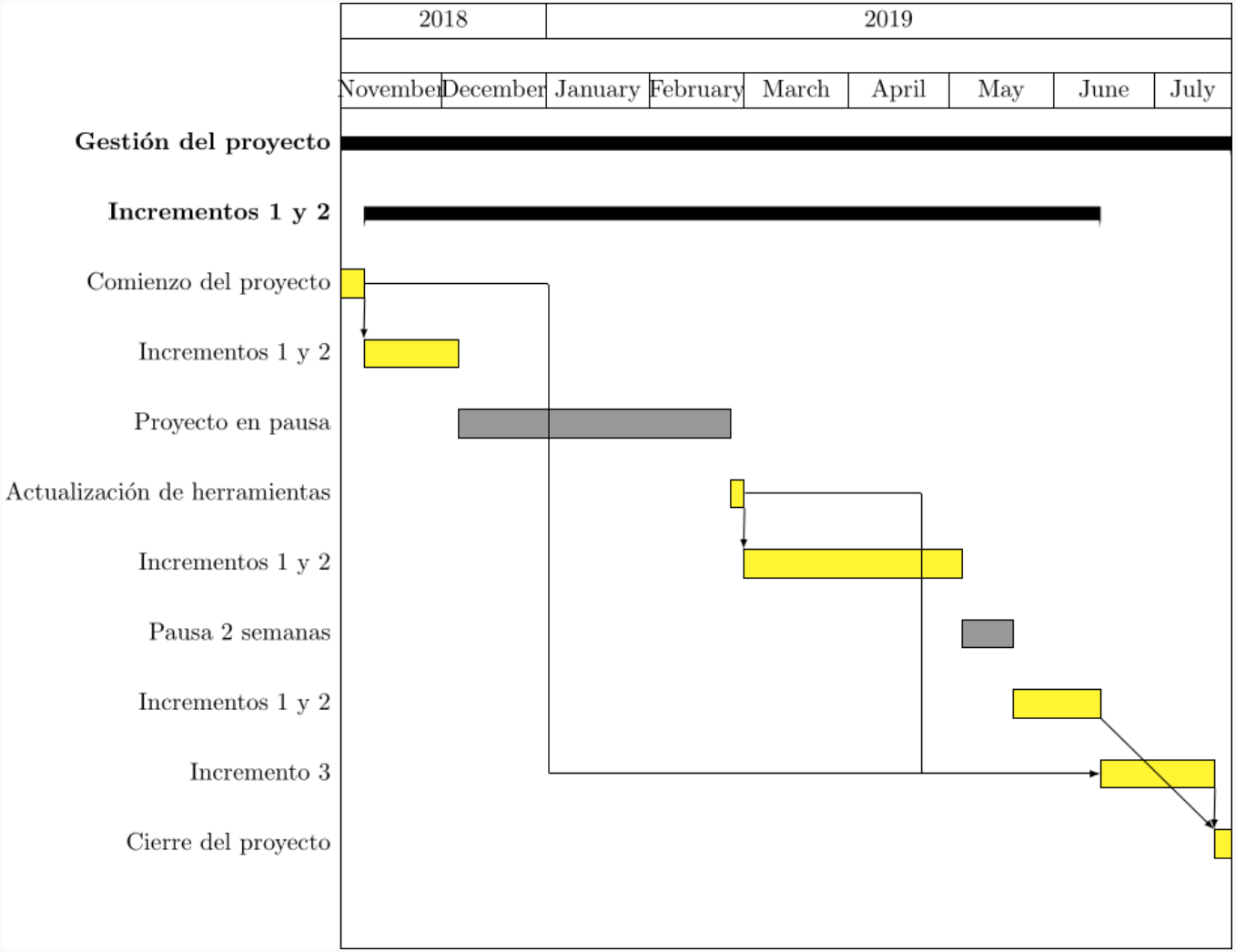




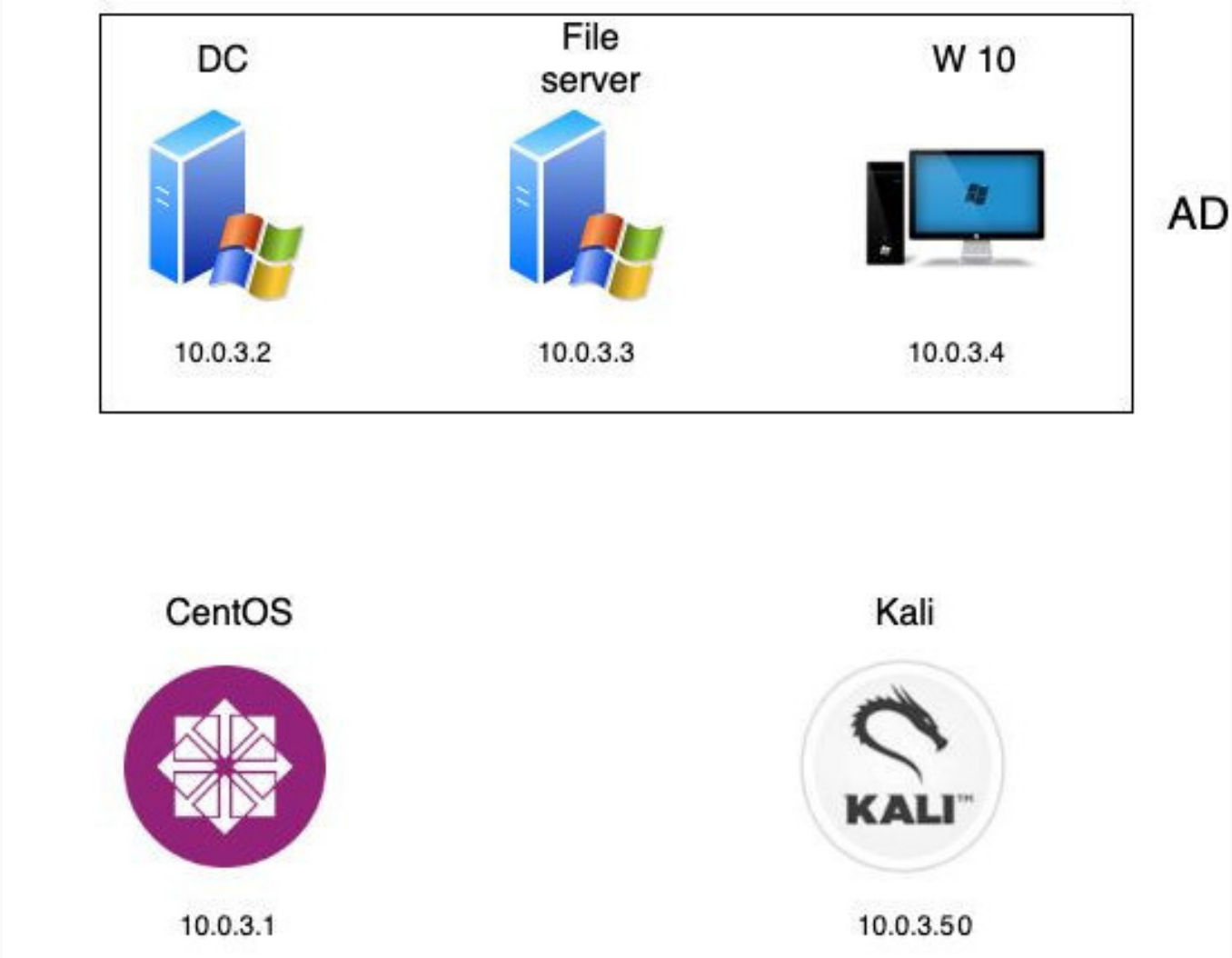
Planificación inicial



Planificación real



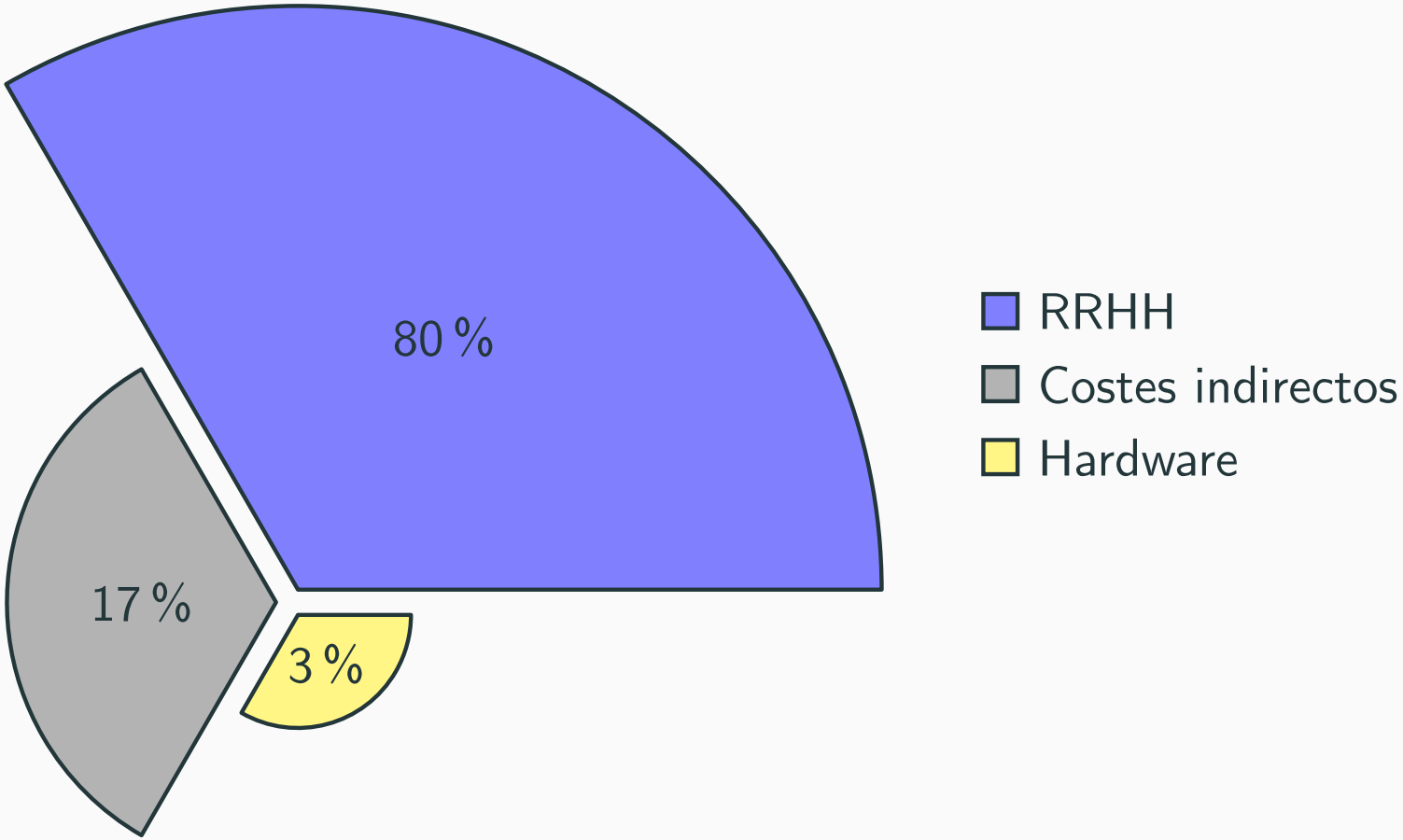
Laboratorio



Gestión de la configuración

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

Estimación de costes



Total: 6072.43€

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€

Tecnologías y herramientas

Desarrollo y configuración principal

Pentesting

Documentación

draw.io

LaTeX

git + GitHub

Vim

GNU Aspell

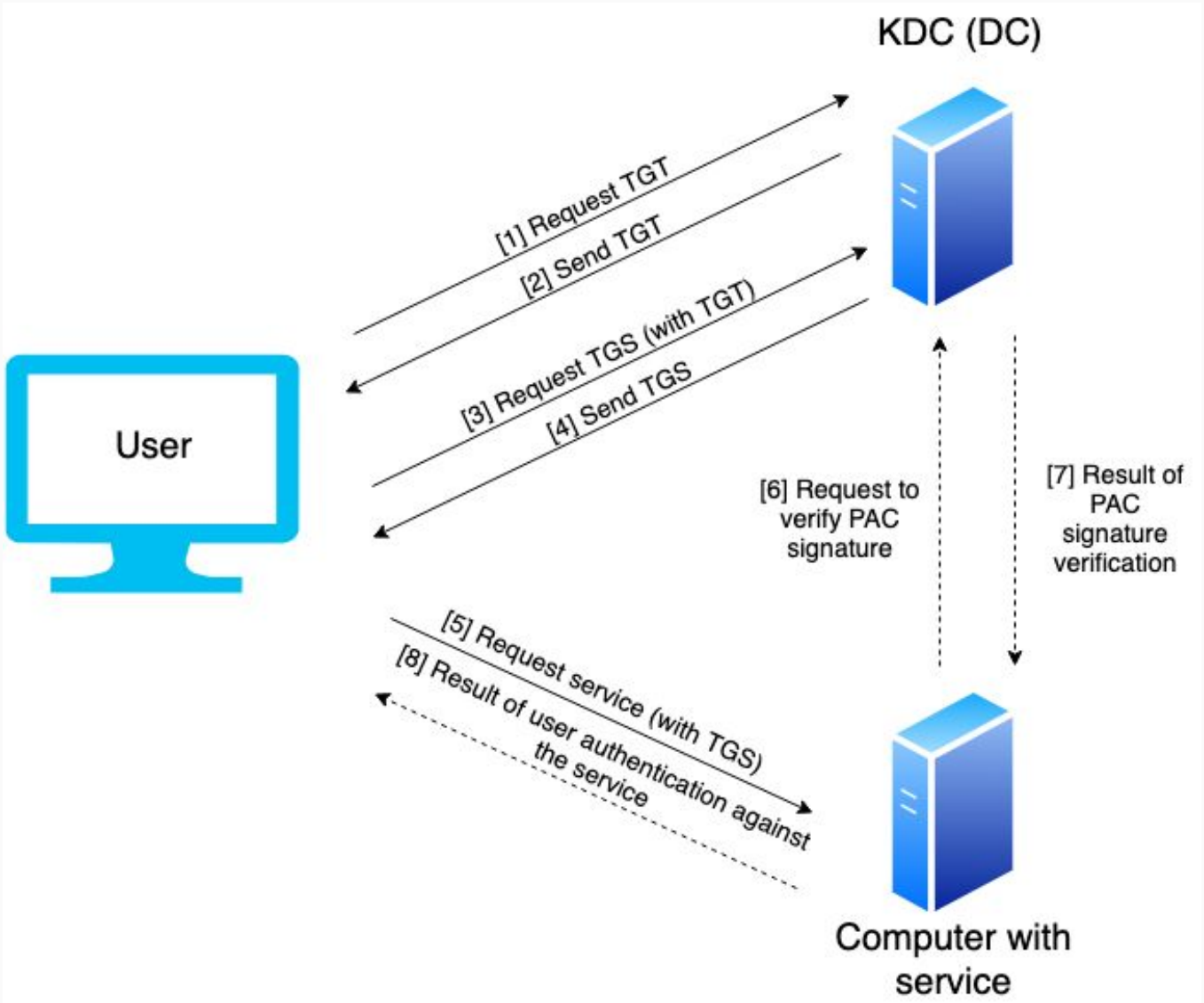
Modelo de trabajo

Modelo de trabajo

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

Incrementos 1 y 2

Golden Ticket



Golden Ticket

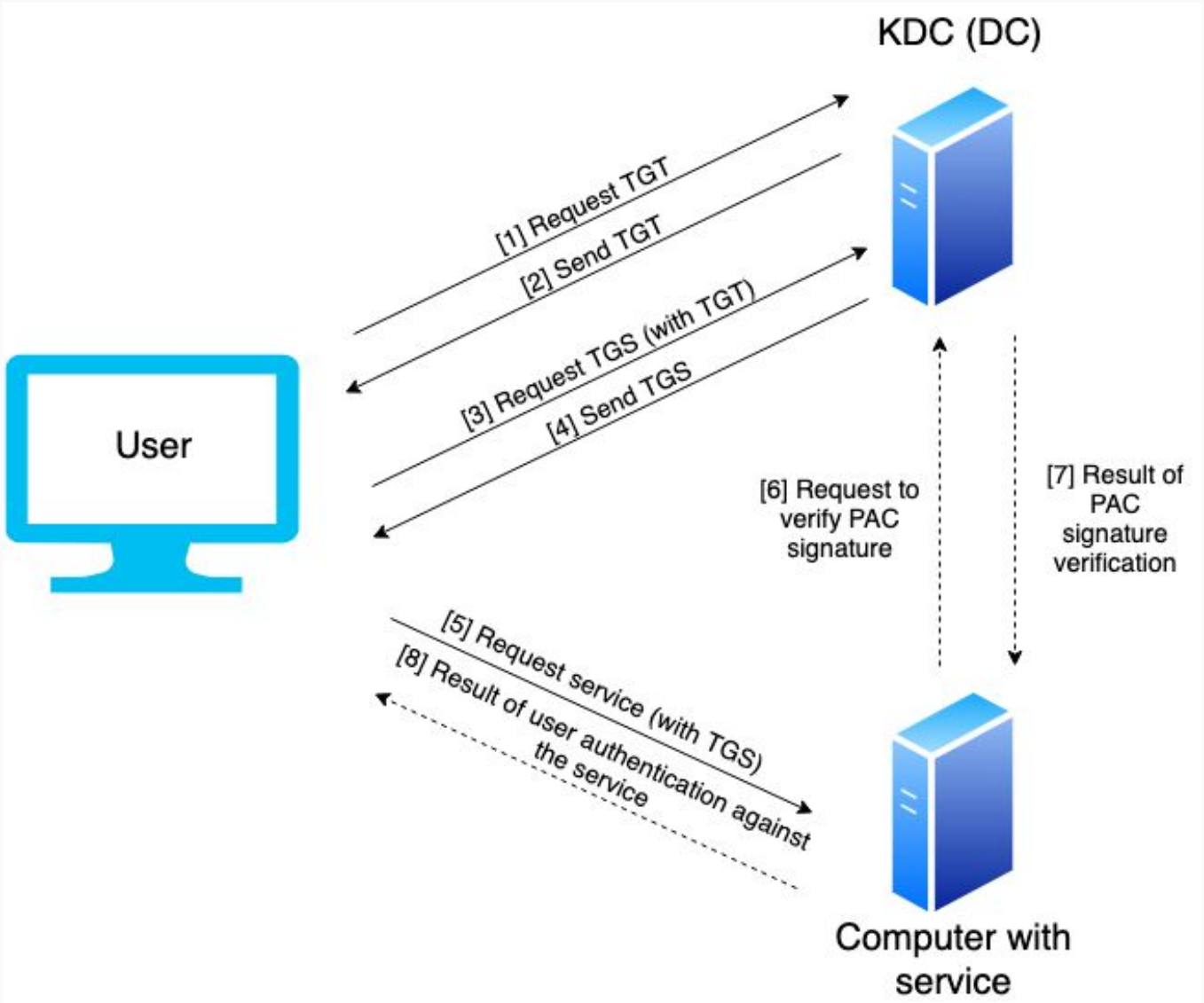
- TGT normal $\rightarrow$ Indetectable.
- Ticket válido hasta:
  - Cambio de contraseña de KRBTGT.
  - Expiración del ticket.

Golden Ticket: Detección

- Programas usados.
  - Técnicas.
  - DLLs.
  - Patrones de texto.

- Uso del ticket.
  - Usuario raro.
  - Longevidad.

Silver Ticket



Extracción de credenciales

- Acceso a archivos clave.
- Volcado de memoria.

PowerShell

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

Logins sospechosos

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

Incremento 3: Ransomware

Ransomware

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

Crypto ransomware: defensa

- 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

Conclusiones

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

Trabajo futuro

- 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

Tutores:
Purificación Cariñena Amigo
Andrés Tarascó Acuña