Universitat Oberta de Catalunya

uoc.edu

Soluciones Endpoint Detection and Response Open-Source

Estado del arte, propuesta de medición, análisis y evaluación para determinar su implementación y aplicabilidad en ambientes empresariales

Jaime Andrés Bello Vieda
Máster en Seguridad de la Información y de las Comunicaciones - MISTIC
Trabajo final de Máster - Hacking

Víctor García Font
Manuel Jesús Mendoza Flores

31 de diciembre, 2019

Agradecimientos:
A Dios,
Gracias por restaurarme, por las personas que has puesto en el camino, por tomarme de la mano y guiarme con tu espíritu.

A mis padres,
Soy lo que soy y lo que no por ustedes,
con aciertos y desaciertos... siempre humano.

FICHA DEL TRABAJO FINAL

Título del trabajo:	Soluciones Endpoint Detection and Response Open-Source Estado del arte, propuesta de medición, análisis y evaluación para determinar su implementación y aplicabilidad en ambientes empresariales
Nombre del autor:	*Jaime Andrés Bello Vieda*
Nombre del consultor/a:	*Manuel Jesús Mendoza Flores*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	12/2019
Titulación:	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones*
Área del Trabajo Final:	*TFM - Hacking*
Idioma del trabajo:	*Castellano*
Palabras clave	*EDR, Endpoint, Ciberataque*

Resumen del Trabajo:

La tendencia año a año de amenazas cibernéticas que han impactado grandes compañias con perdidas económicas considerables, han permitido la aparición de nuevas soluciones que juegan un papel indispensable a la hora de detectar, mitigar y erradicar incidentes como parte de una estrategia y una postura robusta de defensa cibernética; los Endpoint Detection and Response (EDR).

Gartner, una entidad reconocida en asesoramiento de tipo estratégico, menciona que un EDR es una solución de seguridad que registra y almacena el comportamiento de un Endpoint (Como una estación de trabajo o servidores), utilizando diversas técnicas de análisis de datos para detectar comportamientos sospechosos, suministrar información contextual, bloquear actividades maliciosas y proporcionar sugerencias de remediación en sistemas afectados.

El trabajo presenta el estado del arte de aquellos sistemas que pueden asimilarse a una solución de tipo EDR de tipo open-source, y la implementación práctica de un espectro de estos (Proof of Concept - PoC), para observar el funcionamiento y capacidades frente a un sistema víctima infectado con malware reciente tipo Emotet.

Se propone una escala de medición y una evaluación de las capacidades de estos EDR en relación con las características de un EDR mencionadas por Gartner, con el fin de proporcionar una conclusión del estado de madurez de estas soluciones libres como parte de implementaciones reales en la empresa,

proporcionando un marco de trabajo con el cual se puedan medir y evaluar estos sistemas, además de las oportunidades de investigación que pueden surgir a través del desarrollo de esta investigación.

Abstract:

The year-by-year trend of cyberthreats has been impacted large companies with considerable money loss, and this have raised the development of new solutions as part of the game with an indispensable role in detecting, mitigating and eradicating incidents as part of a robust and strategic posture on cyber defense; we're talking about Endpoint Detection and Response (EDR).

Gartner, a recognized strategic advisory entity, argues an EDR is a security solution which records and stores the behavior of an Endpoint (such as a workstation or servers), using various data analysis techniques to detect suspicious behavior, provide contextual information, block malicious activities and provide remediation suggestions for affected systems.

The work presents the current state of those systems that can be similar to an EDR type solution in the open-source field, and the practical implementation of a spectrum of these ones through a Proof of Concept (PoC), to observe the operation and capabilities against a victim system infected with a recent Emotet malware.

A measurement scale and an evaluation of the capabilities of these EDRs are proposed in relation to the characteristics of an EDR mentioned by Gartner, in order to provide a conclusion of the maturity status of these free solutions as part of possible implementations in the company, provides a framework to get these systems measured and evaluated, in addition to the research opportunities that may create through the development of this research.

Índice

Lista de ilustraciones

Lista de tablas

1. Introducción

1.1 Contexto y justificación del Trabajo

La tendencia de incidentes de seguridad se percibe en alza, por ejemplo, el Centro Criptológico Nacional (CCN-CERT) de España en su informe "Ciberamenazas y Tendencias 2019", registró una gestión de 38.192 incidentes durante el año 2018, con un incremento en casos de 43,65% respecto a 2017. El estudio resalta que la proliferación y conectividad de dispositivos Internet of Things (IoT)[1] propicia la distribución de código malicioso y de ataques Distributed Denial of Service (DDoS)[2], siendo facilitadores de la problemática relacionada al incremento incidentes. Flagelos emergentes que persiguen beneficios económicos como el cryptojacking[3], y el asedio en la red de múltiples variantes de ransomware[4], hacen parte del panorama actual en el que los riesgos de ciberseguridad se materializan, afectando a individuales y sectores industriales.

Por otra parte, las repercusiones y pérdidas económicas a raíz de un incidente cibernético son considerables. Estudios e informes recientes cuyas mediciones se realizan a nivel global, como el "Costo de una brecha de datos"[5], que ha venido realizando desde hace más de 10 años el Ponemon Institute e IBM y que condensa los resultados de entrevistas con más de 500 compañías alrededor del mundo que han experimentado y enfrentado incidentes de seguridad, concluye en su versión 2019:

- En promedio, la pérdida económica por una brecha de seguridad es de USD $3.92M.
- En promedio, el tiempo para identificar una brecha es de 206 días, mientras que, para contenerlo es de 73 días; con un ciclo[6] total de 279 días.
- Las brechas de datos causadas por un ataque malicioso cuestan un 27% más en comparación con las relacionadas a errores humanos ($4.45M vs. $3.5M).
- El sector salud representó la industria más afectada por las repercusiones de un incidente, seguida por el sector financiero y de tecnología que ocupan la segunda y tercera posición respectivamente.

[1] Internet de las cosas, puede definirse como un paradigma y desarrollo en el que los objetos cotidianos poseen conectividad de red, permitiéndoles envío/recepción de flujos de datos.
[2] Ataque distribuido de denegación de servicio, es un tipo de ataque dirigido sobre un objetivo puntual por parte de un conjunto de sistemas o red que causa la indisponibilidad o funcionamiento regular del objetivo atacado.
[3] Uso del procesamiento y potencia de cálculo de sistemas informáticos de terceros de manera no autorizada para el minado y resolución de transacciones efectuadas entre criptomonedas.
[4] Amenaza de código malicioso que cifra e impide o restringe el acceso a archivos de un sistema informático, permitiendo de nuevo su acceso al recibirse una llave de descifrado una vez se consiente un rescate o intercambio económico por obtener dicha llave.
[5] Una brecha (O en algunos casos traducido como violación) de datos, se define como un incidente en el que datos sensibles de un individuo (Como información personal, un registro médico, o información financiera) están potencialmente en riesgo.
[6] El reporte denomina a esta sumatoria, ciclo de vida de la brecha de datos.

Con el fin de mitigar y reducir los daños producidos por una amenaza de seguridad, el estudio recomienda la creación de un equipo de respuesta a incidentes[7] y la implementación de tecnologías que mejoren la habilidad de detección y contención de una brecha de seguridad.

Las necesidades de un equipo de respuesta a incidentes

Un equipo de respuesta a incidentes es organizado comúnmente en situaciones puntuales, es decir cuando el incidente está en curso o sus repercusiones ya son percibidas (O sufridas) por la empresa, las personas que conforman equipos tienen algunos conocimientos de seguridad informática y poseen roles de administración y control de sistemas; sin embargo, no cuentan necesariamente con habilidades específicas en respuesta a incidentes.

Dado el impacto de incidentes cibernéticos a gran escala en diversas industrias, se ha creado la necesidad (Por estrategia de la empresa o por el surgimiento de legislación sobre el tema) de implementar equipos permanentes de respuesta a incidentes, estrategia que apalanca una visión proactiva de amenazas antes que surja una crisis en términos de ciberseguridad.

Las organizaciones se están viendo avocadas a evolucionar de esta visión reactiva en cuanto a gestión y respuesta a incidentes se refiere, en la cual el equipo se conforma y actúa por una alerta o notificación externa por parte de un organismo de aplicación de la ley (Policial u otros)[8], a buscar y propender por convertirse en una organización proactiva y guiada/dirigida hacía la caza de amenazas (Threat hunting), a través de un equipo en permanente búsqueda de actividad maliciosa, patrones de red sospechosos y variantes de malware.

Implementación de tecnologías en respuesta a incidentes

Un requisito para la detección, contención y erradicación de una amenaza cibernética es dotar a la empresa, y al equipo de respuesta a incidentes, de visibilidad sobre los activos tecnológicos de la compañía, permitiéndoles conocer cuál es el comportamiento de los puntos finales (En adelante Endpoints) en tiempo real, proporcionando los datos y la inteligencia suficiente en momentos de crisis que permitan la toma de decisiones y acciones en el menor tiempo posible, esta visibilidad y oportunidad de acción se hace posible a través de la implementación de herramientas focalizadas en detección de amenazas y respuesta ante incidentes, destacándose la familia emergente de tecnología conocida como Endpoint Detection and Response (EDR), solución que garantiza monitoreo, contención y erradicación ante las formas de ataque más sofisticadas conocidas actualmente, como el “fileless” malware, uso de funcionalidades como Powershell, WMI[9], y formas avanzadas de inyección de código y ofuscación que escapan a soluciones basadas en firmas y de detección de amenazas en disco.

[7] Se destaca como una de las principales contramedidas al respecto, reduciendo el costo en aproximadamente USD $360.000 el impacto de una brecha de seguridad.
[8] O en casos más curiosos, a través de quejas de usuarios en redes sociales relacionadas principalmente a problemas de disponibilidad.
[9] Windows Management Instrumentation

Gartner Group (En adelante Gartner) define el mercado de los EDR como “soluciones que registran y almacenan el comportamiento a nivel del Endpoint, utilizan diversas técnicas de análisis de datos para detectar comportamientos sospechosos del sistema, suministrar información contextual, bloquear actividades maliciosas y proporcionar sugerencias de remediación para restaurar sistemas afectados”. Las soluciones EDR deben cumplir las siguientes cuatro funcionalidades:

1. Detectar incidentes de seguridad
2. Contener el incidente en el Endpoint
3. Investigar incidentes de seguridad
4. Brindar orientación de remediación

Comercialmente existen diversas opciones que puede tomar una organización al adquirir un EDR, desarrolladas por compañías de la industria con gran experiencia en materia de ciberseguridad y que gozan de buena reputación y reconocimiento en respuesta a incidentes garantizando la calidad de sus productos y soluciones. Sin embargo, la comunidad de seguridad ha aportado importantes alternativas de uso libre y open-source en todo tipo de sistemas y a diversos niveles, con el fin de apoyar la construcción colectiva de conocimiento y brindar una visión de la tecnología sin costo y al alcance de todos.

La presente investigación, busca proporcionar una perspectiva a los sistemas EDR open-source, y a través de una revisión del estado del arte, establecer aquellos más representativos para ser analizados y evaluados mediante una prueba de concepto (Proof of Concept – PoC), con el fin de proporcionar con la experimentación de su operación y capacidades, conclusiones en el cumplimiento de las cuatro funcionalidades definidas por Gartner para este tipo de soluciones de seguridad.

1.2 Objetivos

1.2.1 Objetivo general

Presentar una perspectiva teórico-práctica de los sistemas de respuesta a incidentes Endpoint Detection & Response EDR cuyo desarrollo es open-source y están disponibles para implementación libre; con el fin de proporcionar información de sus capacidades y servir como marco de referencia que determine su suficiencia de acuerdo con los criterios definidos por Gartner para este tipo de tecnologías.

1.2.2 Objetivos específicos

- Analizar el estado del arte a la actualidad de los proyectos y soluciones EDR que se han impulsado por la comunidad de seguridad en general, y grupos de desarrollo de estas tecnologías sin ánimo de lucro.
- Identificar los sistemas EDR open-source más representativos y evaluados como maduros dentro de la investigación y desarrollo del estado del arte, para su selección e implementación en laboratorio.
- Conocer la arquitectura de los sistemas EDR open-source seleccionados para implementación y experimentación de capacidades en ambiente de laboratorio.
- Construir e implementar a nivel práctico los EDR open-source seleccionados para análisis.
- Probar los EDR implementados mediante la infección deliberada de un sistema con malware para verificar la funcionalidad detección y posibilidad de repuesta de los EDR.
- Proporcionar una conclusión de los EDR respecto a las funcionalidades determinadas por Gartner como resultado de la prueba de concepto PoC y testeo efectuados sobre éstos.
- Exponer las conclusiones y oportunidades futuras de desarrollo adicionales que puedan crearse fruto del desarrollo de este trabajo.

1.3 Metodología

Definición del plan de trabajo
Se recopila la información del contexto actual para identificar y delimitar la problemática planteada de manera que se sustente la necesidad de efectuar la investigación. Teniendo este marco conceptual, se definen los objetivos, la metodología a seguir para desarrollarlos, la estructura de desglose de trabajo (EDT), se determinan los riesgos y la enumeración de hitos a través de los entregables.

Análisis conceptual y del estado del arte
Mediante la recopilación y análisis de la información obtenida se procede a profundizar en el estudio del estado del arte, para entender con mayor detalle los desarrollos EDR open-source de implementación libre más reconocidos en la actualidad, identificando así las similitudes y diferencias preliminares entre ellos, para determinar los más representativos[10] tratándolos en fases posteriores mediante implementación y desarrollo de experimentos con una PoC usando variantes de software malicioso (malware).

Requisitos para la implementación de EDRs open-source
Análisis de los requisitos para la implementación de los EDR open-source seleccionados a estudio en este trabajo, definición del ambiente de laboratorio y recursos necesarios de procesamiento, dependencias de software, instalación de componentes, herramientas o módulos de terceros, entre otros.

Implementación de EDRs open-source
Etapa en la cual se efectuará la instalación y configuraciones correspondientes para los sistemas EDR open-source, con el fin de ponerlos a punto y funcionales para la PoC mediante un testeo con malware.

PoC y mediciones de características Gartner
Se pretende evaluar las herramientas EDR y su operación frente a un sistema monitoreado y deliberadamente infectado con malware como PoC con el fin de experimentar, y obtener conclusiones y ponderaciones frente a las funcionalidades enunciadas por Gartner que deben cumplir este tipo de sistemas de detección y respuesta a amenazas de seguridad.

Conclusiones y oportunidades
En esta etapa final, a través de un análisis sobre la ejecución del trabajo realizado, se presentarán las conclusiones referentes a la utilidad potencial de los sistemas EDR open-source objeto de este estudio para ser implementadas como una solución de detección, monitoreo y respuesta ante incidentes en el ambiente productivo de una organización, además de resaltar las oportunidades y líneas futuras de investigación que pueden derivarse o profundizarse tomando como punto de partida este trabajo final de máster.

[10] En este apartado no se habla de un alcance específico en cuanto a la cantidad de sistemas a seleccionar para analizar, durante el proceso de investigación se concluirán los sistemas a analizar, tomando en cuenta esta información, y las limitaciones en tiempo para el desarrollo total de este Trabajo Final de Máster.

1.4 Listado de tareas

Como parte del alcance y detalle de los componentes de desarrollo de esta investigación, se ha desarrollado una EDT, herramienta usada en la gestión de proyectos que orienta los entregables PEC a lo largo del desarrollo del trabajo.

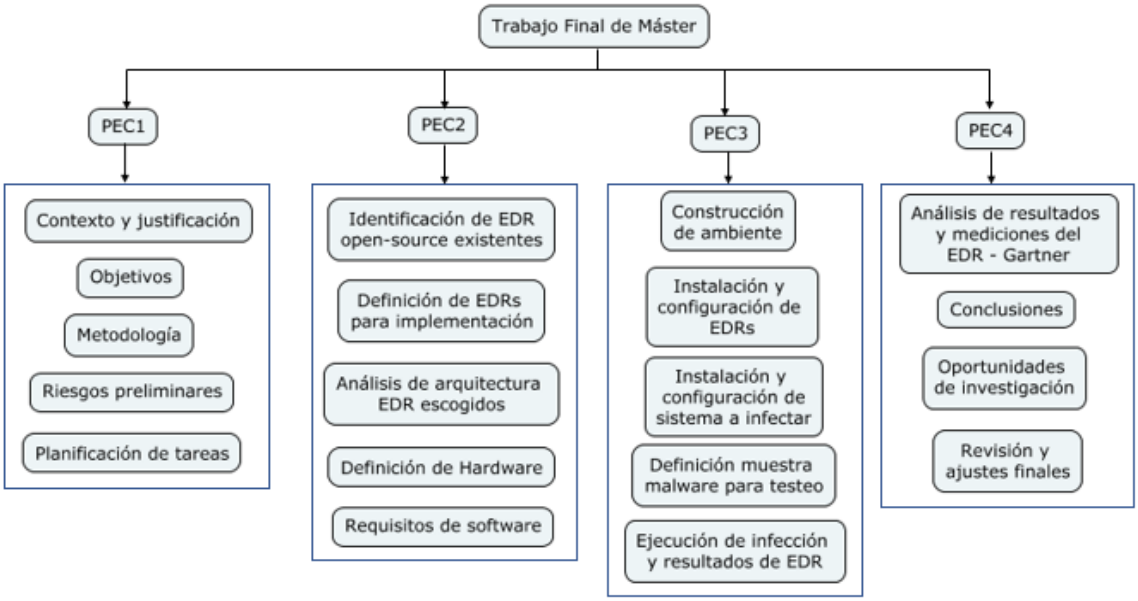


Ilustración 1. Estructura de desglose de trabajo TFM.

En esta EDT solo se detalla el trabajo necesario para completar el TFM, siendo la entrega 5 (Video) parte de la sustentación final del mismo luego de su desarrollo final.

PEC1 – Plan Trabajo

Punto de control en el que se presenta la planificación para el desarrollo del trabajo, consta de los siguientes aspectos para su obtención:

- Contexto y justificación: Se describe la situación actual por la cual se crea la necesidad de desarrollar una investigación alrededor del tema.
- Objetivos: Se trazan los elementos a alcanzarse a través del desarrollo del trabajo.
- Metodología: Se describen las diferentes fases que serán abordadas para generar el contenido teórico suficiente que permita pasar al desarrollo de un experimento práctico y obtener conclusiones.
- Listado de actividades (EDT): Trabajo necesario para alcanzar los objetivos propuestos.
- Riesgos preliminares: Enumeración de los riesgos que pueden impactar el desarrollo, resolución de las actividades y por ende los objetivos del trabajo.
- Planificación de tareas: Estimación temporal de las actividades específicas a desarrollar dentro del calendario en que está establecido el desarrollo general del proyecto y los hitos (puntos de control) a través de la entrega de las PEC.

PEC2 – Estado del arte y definición de sistemas EDR para PoC
Hito en el cual se desarrolla una investigación teórica del tema, se llevan a cabo indagaciones sobre los trabajos y avances alcanzados en torno al tema de estudio, se analiza la información obtenida, se identifican los sistemas más representativos del caso, y se toma una decisión para profundizar sobre éstos.

- Identificación de EDR open-source existentes: Revisión de los proyectos y soluciones existentes al interior de la comunidad abierta de seguridad, fuentes de investigación académica, agremiaciones de tecnología e Internet.
- Definición de EDRs para implementación: Escogencia de los sistemas EDR open-source más robustos desarrollados, para continuar una revisión en detalle de estos.
- Análisis de arquitectura EDR escogidos: Revisión del diseño de sistemas EDR, y los componentes y módulos que lo integran con el fin de establecer una idea preliminar de requerimientos en hardware/software, de cara a la implementación práctica de estos.
- Definición ambiente de laboratorio (Hardware): Establecimiento de requisitos de infraestructura y procesamiento para establecer el ambiente de laboratorio de experimentación.
- Requisitos de software: El software, paquetes, módulos, scripts y componentes de terceros necesarios para la instalación y configuración del ambiente de laboratorio del trabajo y la implementación de los EDR escogidos.

PEC3 – Implementación de EDRs y PoC
Entrega sobre el componente de experimentación del tema de estudio, a través de la instalación y configuración del ambiente de laboratorio y ejecución de la PoC.

- Construcción de ambiente para experimentación: Configuración de hardware y montaje de infraestructura para instalación de software.
- Instalación y configuración de EDRs: Proceso y consecución de ejecución de scripts, paquetes y software necesario para obtener los sistemas EDR escogidos.
- Instalación y configuración de sistema a infectar: Instalación de un sistema de cómputo para ser infectado como parte de la PoC de testeo de los EDR.
- Definición muestra malware para testeo: Análisis para determinar una amenaza que pueda ser interesante de usar para probar el funcionamiento y efectividad en detección y respuesta por los EDR de la PoC.
- Ejecución de la infección y resultados obtenidos por los EDR: Verificación de la operación del EDR luego de ejecutar deliberadamente la amenaza maliciosa sobre el sistema anfitrión que será infectado.

PEC4 – Redacción memoria final
Entregable que representa la integración completa de información y trabajo desarrollado en el TFM, incluyéndose las conclusiones y oportunidades futuras de desarrollo o investigación sobre el tema de estudio.

- Análisis de resultados y mediciones del EDR con Gartner: Comparación de acuerdo con los resultados de la experimentación de los EDR implementados y sus capacidades, frente a las características resaltadas por Gartner que estos sistemas deben cumplir.
- Conclusiones: Resultados finales fruto del análisis teórico y ejecución práctica del trabajo de investigación.
- Oportunidades de investigación: Se proporcionan ideas que pueden apoyar nuevas líneas de investigación sobre la temática en que se enmarcó el presente trabajo, o, por otra parte, profundizar sobre un complemento que contribuya a un desarrollo y alcance adicional sobre el mismo.
- Revisión y ajustes finales: Lectura y análisis final del TFM con los ajustes de forma y estructura correspondientes.

Entrega5 – Presentación en video
Desarrollo de una exposición sobre el trabajo, presentándose a través de un video para ser entregado como soporte de la investigación desarrollada y como insumo para la valoración del tribunal de evaluación asignado.

- Esquema del contenido del video: Selección de contenido del video
- Elaboración de la presentación y material de apoyo: Realización de la presentación
- Grabación del video

Defensa trabajo máster

- Periodo para la resolución de inquietudes, aclaración de dudas y demás cuestiones que puedan surgir por parte del tribunal encargado del análisis y evaluación del trabajo.

1.5 Riesgos preliminares

Sobredimensión del alcance: La estructura inicial del proyecto cubre un conjunto demasiado grande respecto a las limitaciones de tiempo y calendario establecidas (Aproximadamente 3 meses y medio).

Falta de información para el desarrollo de la investigación: Dificultad en la identificación de información sobre los temas o áreas planteadas en el trabajo a nivel teórico como de implementación práctica, como manuales, tutoriales y otros que soporten la construcción e implementación de los EDR a nivel práctico.[11]

Dificultades en la construcción de sistemas: Errores no esperados durante la instalación de software, módulos, paquetes entre otros para la puesta a punto de los EDR y su integración con el sistema a infectar para la PoC.

[11] Al tratarse de una investigación sobre tecnologías no comerciales, que son desarrolladas y soportadas por colaboradores de la comunidad de seguridad.

1.6 Planificación

A continuación, se encuentra la planificación temporal de actividades mediante un diagrama de Gantt.

ACTIVITY	DURATION (DAYS)
Trabajo Final de Máster	3
Contextualización sobre la materia UOC	1
Pautas para el desarrollo del trabajo (Lectura de Iria da Cunha)	2
Plan de trabajo	10
Contexto y justificación	3
Objetivos	2
Metodología	4
Listado de actividades (EDT)	4
Riesgos preliminares	1
Planificación de tareas	6
Estado del arte y definición de sistemas	22
Identificación de EDR open-source existentes	7
Definición de EDR para implementación	4
Análisis de arquitectura EDR escogidos	7
Definición ambiente de laboratorio (Hardware)	3
Requisitos de software	3
Implementación de EDRs y PoC	28
Construcción de ambiente para experimentación	6
Instalación y configuración de EDRs	6
Instalación y configuración de sistema a infectar	4
Definición muestra malware para testeo	6
Ejecución de la infección y resultados obtenidos por los EDR	6
Redacción memoria final	31
Análisis de resultados y mediciones del EDR con Gartner	10
Conclusiones	5
Oportunidades de investigación	4
Revisión y ajustes finales	17
Presentación en video	5
Esquema del contenido del video	1
Elaboración de la presentación y material de apoyo	2
Grabación del video	2

Ilustración 2. Planificación de actividades

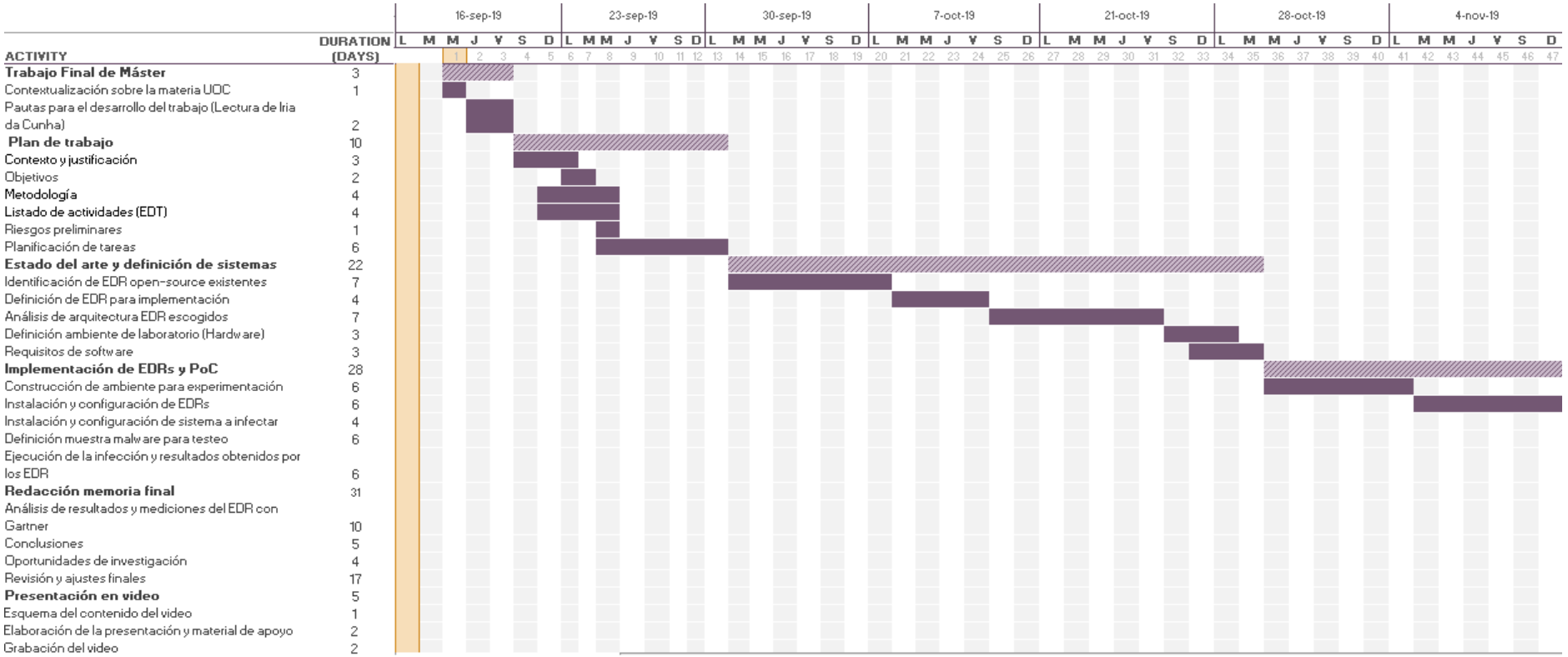
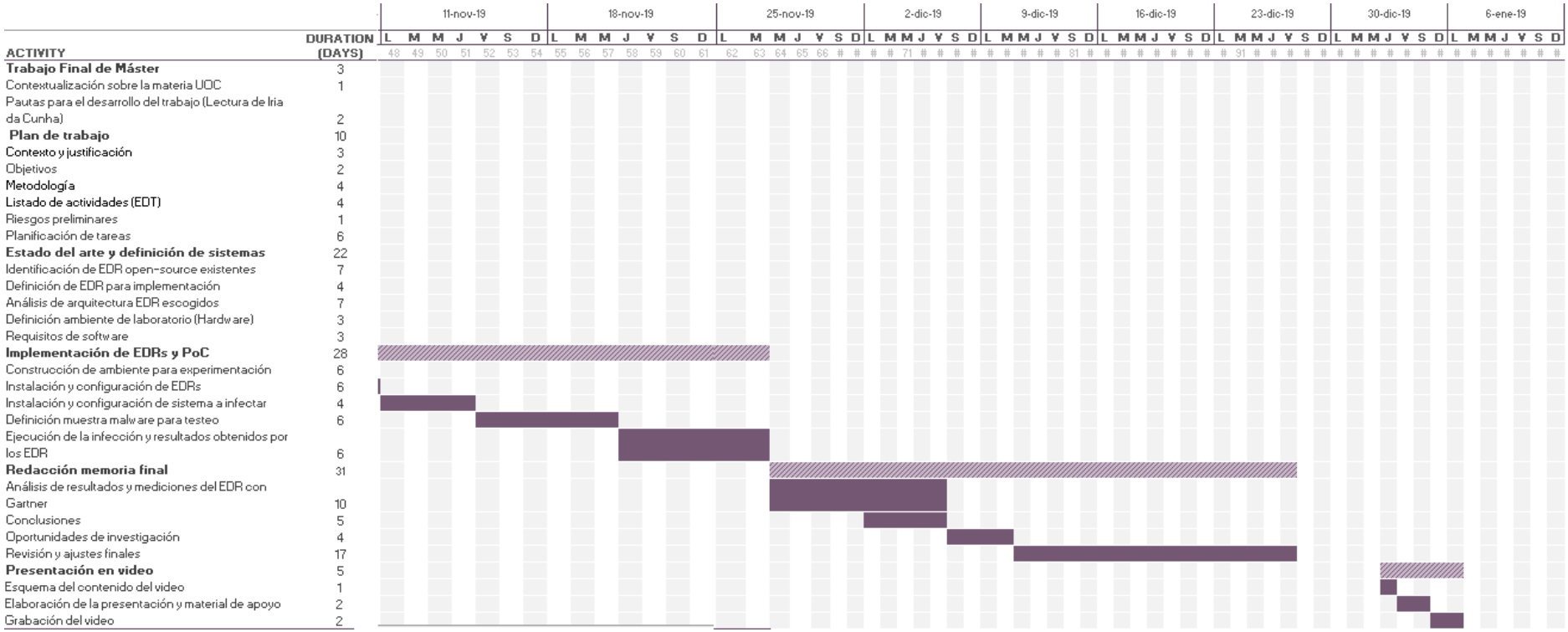


Ilustración 3. Diagrama de Gantt (Parte 1)



ACTIVITY	DURATION (DAYS)
Trabajo Final de Máster	3
Contextualización sobre la materia UOC	1
Pautas para el desarrollo del trabajo (Lectura de Iria da Cunha)	2
Plan de trabajo	10
Contexto y justificación	3
Objetivos	2
Metodología	4
Listado de actividades (EDT)	4
Riesgos preliminares	1
Planificación de tareas	6
Estado del arte y definición de sistemas	22
Identificación de EDR open-source existentes	7
Definición de EDR para implementación	4
Análisis de arquitectura EDR escogidos	7
Definición ambiente de laboratorio (Hardware)	3
Requisitos de software	3
Implementación de EDRs y PoC	28
Construcción de ambiente para experimentación	6
Instalación y configuración de EDRs	6
Instalación y configuración de sistema a infectar	4
Definición muestra malware para testeo	6
Ejecución de la infección y resultados obtenidos por los EDR	6
Redacción memoria final	31
Análisis de resultados y mediciones del EDR con Gartner	10
Conclusiones	5
Oportunidades de investigación	4
Revisión y ajustes finales	17
Presentación en video	5
Esquema del contenido del video	1
Elaboración de la presentación y material de apoyo	2
Grabación del video	2

Ilustración 4. Diagrama de Gantt (Parte 2)

1.7 Productos obtenidos

Apoyado en la EDT desarrollada para el desarrollo del TFM, los productos obtenidos que conforman el resultado final del proyecto son:

PEC1: Que condensa el plan de trabajo, donde se define la manera y guía en que será desarrollado el TFM.

PEC2: Que presenta el estado del arte del tema y un análisis puntual de los sistemas EDR escogidos para las etapas prácticas del trabajo.

PEC3: Donde se expresan los resultados sobre la etapa práctica y de experimentación de los EDR y el desarrollo de la PoC para observar las capacidades y rendimientos de estos.

PEC4: Compendio de entregas PEC desarrolladas a lo largo del TFM, incluyendo las conclusiones y trabajo futuro que puede establecerse alrededor del mismo.

Entrega 5: Elaboración de material de apoyo y desarrollo de un video sobre el trabajo, donde se sustentan los componentes más relevantes de la investigación y sus conclusiones.

2. ¿Qué es un Endpoint?

Para muchos profesionales de tecnología y que se desempeñan en el campo de la seguridad de la información, una definición común de Endpoint es “Cualquier cosa con un teclado”. No obstante, la evolución digital ha traído consigo un mundo móvil e interconectado, que incluye dispositivos personales, máquinas virtuales, terminales de punto de venta (POS – Point-of-sale), unidades del Internet de las Cosas (IoT – Internet of Things) y sistemas industriales del mundo OT[12], entre otros.

Con la inclusión de estas nuevas tecnologías, esta definición puede extenderse como “Cualquier dispositivo con capacidades de poseer una dirección IP permitida para interactuar al interior de una organización”.

La figura ilustra la jerarquía de dispositivos y el valor de negocio que estos representan comúnmente para una organización[13]; la base de la pirámide representa los dispositivos de usuario final como equipos de escritorio o portátiles que pueden llegar a ser menos sensible que un servidor, por ejemplo.

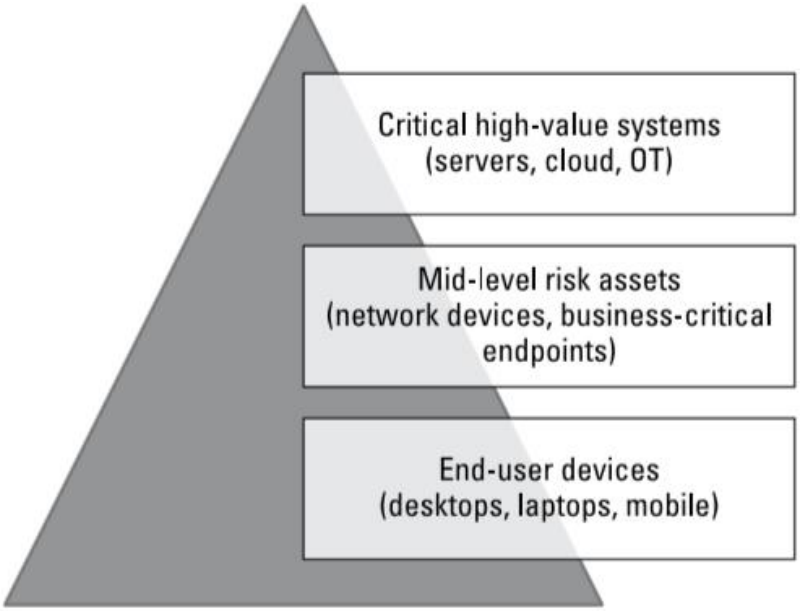


Ilustración 5. Pirámide de activos tecnológicos y valor de negocio

Se debe destacar la necesidad de protección y monitoreo a lo largo de todos los sistemas que conforman esta pirámide, que en su conjunto conforman lo que puede denominarse como un Endpoint, todos ellos traen consigo riesgos que pueden llevar a escenarios en que, a través del compromiso de una amenaza en un activo de menor valor estratégico, puede convertirse un punto de pivote o salto hacía activos más sensibles.

[12] Operation Technology. Se conoce con este concepto al hardware y software dedicado al control y cambios de dispositivos físicos como válvulas, tuberías, compuertas de sistemas industriales como el SCADA (Supervisory Control and Data Acquisition).
[13] Ilustraciones 5 y 6 tomadas del libro Endpoint Detection and Response for dummies.

3. Definiendo un EDR

3.1 ¿Qué es y qué función cumple una tecnología EDR?

Endpoint Detection and Response, conocido en el mundo de la tecnología con el acrónimo EDR, se ha convertido rápidamente en un método para identificar y responder a amenazas en el entorno computacional de una organización. La compañía de investigación y consultoría Gartner define EDR como “soluciones que registran y almacenan el comportamiento a nivel del Endpoint, utilizan diversas técnicas de análisis de datos para detectar comportamientos sospechosos del sistema, suministrar información contextual, bloquear actividades maliciosas y proporcionar sugerencias de remediación para restaurar sistemas afectados”. Este tipo de sistemas demandan las siguientes cuatro características ilustradas a continuación, el primer criterio corresponde con la detección, mientras que los otros tres hacen parte de las actividades de respuesta:

- Habilidad de detectar incidentes de seguridad cuando ocurren
    - Detección de incidentes que representen debilidades o detrimento en la seguridad de los Endpoint y que pueden propagarse a otros equipos de la red confirmando violaciones de seguridad, monitoreo de actividades y validando indicadores de compromiso. (IoC).

- Contener el incidente en el/los Endpoint(s)
    - Estrategias que contribuyen a la mitigación del incidente, las cuales pueden ser el bloqueo de ejecución de un proceso, terminar conexiones ip/dominio, aislar el agente, entre otros.

- Soportar la investigación del incidente
    - Proporcionar capacidades adicionales para verificar cambios en integridad de archivos, procesos y actividad que ha ocurrido en el sistema.

- Proporcionar mecanismos para remediar la situación sobre el/los Endpoint(s) afectados
    - Habilidades para remoción de la amenaza en el sistema, como eliminación de archivos, llaves de registro creadas para persistencia, detención (parada) de tareas programadas.

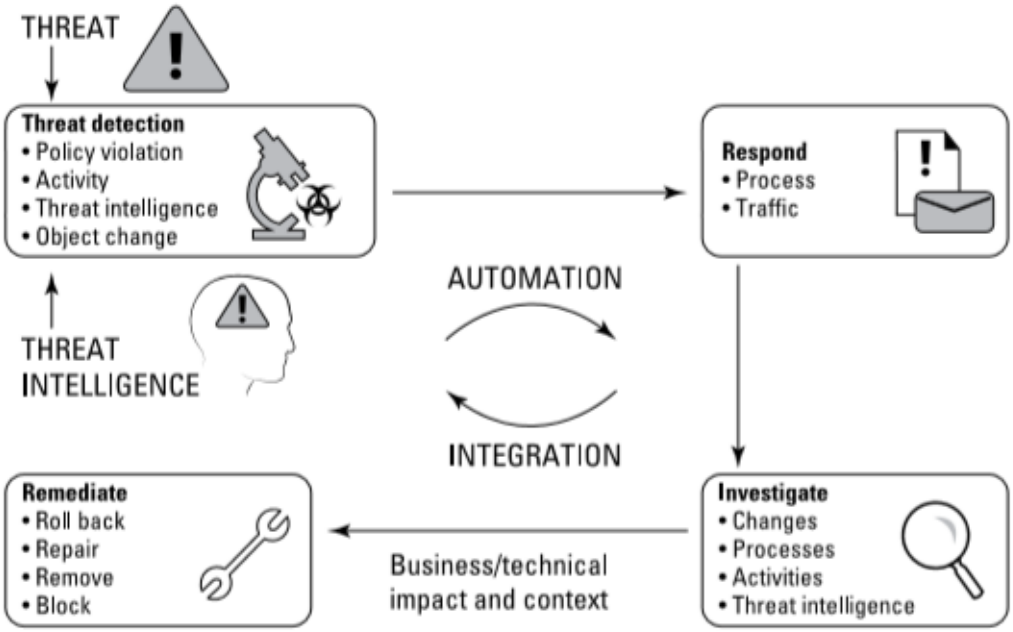


Ilustración 6. Las cuatro capacidades de un EDR

Los sistemas EDR, consiguen a través de un agente de software servicio o similares instalado en los Endpoint, detección de amenazas, supervisión y capacidad recolección de información recibida y procesada de manera centralizada con la cual se realiza análisis del comportamiento, actividades, configuraciones de software, entre otras que ocurren en tiempo real y con las cuales se pueden inferir problemas de seguridad de los equipos monitoreados.

3.2 Panorama actual de soluciones EDR open-source

Dado que las tecnologías EDR son un mercado impulsado y estudiado por grandes casas de tecnología y entidades expertas en la materia vistas anteriormente entre ellas Gartner; se cuenta en Internet y los sitios web de proveedores como CrowdStrike o Carbon Black (Por mencionar algunos) información respecto a las funcionalidades de sus respectivos desarrollos, así como comparaciones con otras opciones similares dentro de este conjunto de soluciones. Esta situación no presenta el mismo escenario para los desarrollos EDR de tipo open-source; durante el desarrollo de esta investigación, se ha llegado a la conclusión que el panorama al respecto se encuentra en estados iniciales, no se observan fuentes variadas de consulta, ni estudios o comparaciones respecto a las herramientas desarrolladas de este tipo.

Si bien la situación expuesta reflejó aparentemente limitaciones por no contarse con fuentes que hablen del tema, aquellos sistemas que poseen funcionalidades que pueden enmarcarse como EDR open-source, cuentan con su presentación como producto y su desarrollo en páginas web propias de estas tecnologías y en repositorios de código abierto como GitHub.

Una de las fuentes iniciales de información respecto a la identificación de soluciones EDR open-source corresponde a un artículo de la empresa Cyberbit escrito durante 2017 y denominado “Top 5 Open Source Incident Response Automation Tools”.

En este recurso, se puede observar la referencia a algunas herramientas y sistemas open-source que automatizan y atienden de manera remota Endpoints asimilándose a soluciones tipo EDR como son:

- CimSweep

Es una suite basada en WMI que posibilita la conducción de tareas relacionadas con respuesta a incidentes y cacería de amenazas de manera remota en sistemas basados en Windows.

El proyecto se encuentra en el siguiente repositorio GitHub https://github.com/PowerShellMafia/CimSweep

- GRR Rapid Response

Es un sistema basado en lenguaje Python y el despliegue de agentes de monitoreo que reportan centralizadamente a un servidor desde el cual es posible el acceso remoto a los Endpoints para desarrollar labores de respuesta a incidentes, posibilita revisión y análisis de archivos y del registro de Windows. La solución cuenta con soporte para Endpoints cliente Windows, Linux y OSX.

El proyecto se encuentra en el repositorio GitHub https://github.com/google/grr, y la documentación en https://grr-doc.readthedocs.io/en/latest/.

- Osquery

Sistema multiplataforma (Windows, Linux, OSX) creado por Facebook que habilita la visión del sistema operativo a través de peticiones o sentencias en lenguaje SQL.

Osquery cuenta con una página web propia del proyecto en https://osquery.io/, el código se encuentra en GitHub en https://github.com/osquery/osquery y la documentación en https://osquery.readthedocs.io/en/stable/.

- MIG

Plataforma creada por Mozilla para el análisis e investigación de Endpoints remotos, se basa en agentes que son instalados sobre la infraestructura que será monitoreada. MIG permite análisis del sistema de archivos, estado de red, configuración y memoria RAM.

Cabe destacar que este proyecto dejó de ser mantenido por Mozilla y tampoco es usado al interior de la compañía, el proyecto y código puede aún ser usado sin mucha garantía de su efectividad dada su falta de soporte. La página oficial del proyecto se encuentra en https://mig.mozilla.org/, su código en https://github.com/mozilla/mig, y la documentación en https://mig.mozilla.org/doc.html.

Finalmente, en este recurso de Internet se mencionaba a TheHive, una plataforma que facilita la creación de casos e investigación de incidentes. Al revisar el proyecto se concluyó que no es una solución pensada para el monitoreo de Endpoints y se pueda tomar como un EDR. No obstante, se incluye ésta como referencia dentro del estado del arte de sistemas open-source orientados a seguridad y respuesta a incidentes. Sitio web propio en https://thehive-project.org/, el código se encuentra en GitHub en https://github.com/TheHive-Project/TheHive y la documentación en https://github.com/TheHive-Project/TheHiveDocs.

Se realizó investigación usando portales reconocidos como el IEEE (Institute of Electrical and Electronics Engineers), ACM (Association for Computing Machinery) entre otras fuentes de información científica y de tecnología con el fin de identificar publicaciones o trabajos desarrollados en este tema sin identificarse información asociada. Navegando en el portal de código libre GitHub y en general a través de Internet se identificaron proyectos adicionales como son:

- Wazuh

Es una evolución del proyecto OSSEC de 2004 que extiende la funcionalidad de este IDS a nivel de host (HIDS o Host Intrusion, Detection System). Hacía el año 2015, el equipo de desarrolló emprendió esfuerzos por lograr una solución de seguridad más completa.

Cuenta con diferentes características como integración con tecnologías de nube de Amazon Web Services (AWS) y Microsoft Azure, además de funcionalidades de respuesta a incidentes valiéndose de Osquery para efectuar peticiones a demanda.

El proyecto cuenta con una web propia en https://wazuh.com/, el código del proyecto en https://github.com/wazuh/wazuh, y la documentación en https://documentation.wazuh.com/3.10/index.html.

- LimaCharlie

Es una plataforma en nube que elimina la necesidad de implementación de infraestructura y mantenimiento. Funciona gracias al despliegue de agentes que son descargados desde la interfaz web e instalados hacía los Endpoint que quieren ser monitoreados, nació como un proyecto open-source hasta transformarse en lo que es a la actualidad; los creadores del proyecto tenían su código en el repositorio GitHub https://github.com/refractionPOINT/limacharlie donde sus creadores mencionan que la versión libre no la pueden mantener y se encuentran en planes de abrir nuevamente el conocimiento a la comunidad abierta de seguridad.

LimaCharlie ofrece diferentes metodologías de pago de acuerdo con las funcionalidades que se requieran habilitar iniciando por un costo de USD $0.50 por agente instalado que ofrece habilidades de detección-respuesta de amenazas y una opción de acceso remoto Live View, que se puede observar

comúnmente en herramientas EDR de tipo comercial y es muy útil para efectuar labores de respuesta ante incidentes. La página oficial es https://www.limacharlie.io/ y su documentación de uso en http://doc.limacharlie.io/en/master/.

- Velociraptor

Es una plataforma open-source enfocada al monitoreo y desarrollo de actividades basadas en forense digital, recolección de información para investigaciones, caza de amenazas y respuesta a incidentes, su arquitectura cliente-servidor permite el monitoreo centralizado de Endpoints, cuenta con soporte para sistemas Windows, Linux y Mac OSX. El motor de reglas empleado para la recolección de información, a diferencia de muchas soluciones que emplean Osquery, es Velociraptor Query Language (VQL) desarrollado por los creadores de la solución. Se percibe como una solución muy similar a GRR expuesta anteriormente. La información sobre este proyecto se encuentra en https://www.velocidex.com/ y su documentación en https://www.velocidex.com/docs/.

4. Herramientas EDR seleccionadas para PoC

Luego de la investigación y una vez identificados y analizadas las herramientas EDR open-source existentes para la comunidad de seguridad, y que pueden ser implementadas y usadas a nivel empresarial, la tabla a continuación presenta cada uno de los sistemas anteriormente enunciados, junto con su justificación de elección o no, con el fin de profundizar sobre estos proyectos y que serán sujetos para la PoC y de experimentación práctica de sus capacidades y funcionalidades.

EDR	Análisis y justificación	Seleccionado
CimSweep	Revisando el proyecto, el desarrollo se percibe como un uso interesante de las funcionalidades WMI de los sistemas Microsoft, esta tecnología comúnmente es utilizada con propósitos maliciosos y como parte de las Tácticas, técnicas y procedimientos (TTP) que se pueden identificar en un ataque informático, con lo cual su uso se convierte de doble propósito (legitimo o ilegitimo) a nivel empresarial. Este proyecto no fue seleccionado para continuar con los propósitos de esta investigación ya que no cuenta propiamente con las habilidades de un EDR en cuanto a identificación, detección, alertamiento de amenazas y otros componentes propios de otros componentes. La suite puede ser útil para labores de respuesta cuando ya está confirmado un incidente o una situación anómala en los Endpoint una vez una herramienta externa avise de la situación. Una desventaja de esta herramienta es que no es multiplataforma, ya que WMI fue desarrollada por Microsoft y solamente cubre sistemas Windows.	✗
GRR Rapid Response	Este sistema de Google se accede a través de una interfaz web que garantiza una visibilidad a nivel gráfico de los Endpoints, es multiplataforma extendiendo sus posibilidades de monitoreo incluyendo sistemas Linux y OSX, es un proyecto que continúa con soporte y mantenimiento y cuenta con una documentación que se percibe bastante robusta respecto a su implementación y utilización. Este sistema ha sido elegido para investigación y para la PoC de este trabajo.	✓
Osquery	Osquery se percibe como una herramienta bastante potente y muchas soluciones EDR tanto comerciales como open-source se basan en ella para realizar peticiones hacía los Endpoints, sin embargo, esta solución corresponde a la instalación de los agentes o clientes de monitoreo que pueden ser llamados remotamente por la integración de otros sistemas como Fleet y que se encuentra documentada en un paper de investigación del SANS Institute "Exploring Osquery, Fleet, and Elastic Stack as an Open-source solution to Endpoint Detection and Response". El análisis de esta solución vale la pena por la integración de estos componentes con el fin de construir un EDR, sin embargo, en razón a las acotaciones tiempo establecidas para el desarrollo de este trabajo, no será incluido para el desarrollo de la PoC. Una solución que integra estas tecnologías será tratada dentro del análisis detallado.	✗
MIG	No se tomará en cuenta para revisarse en detalle por ser un proyecto que, al no continuar con actualizaciones y soporte, puede representar problemas en su implementación, además que el proyecto en este estado sería de difícil adopción en el entorno empresarial productivo de una empresa.	✗

WAZUH	El análisis del proyecto y su documentación expone que WAZUH es una herramienta bastante robusta de seguridad que posee capacidades de identificación, detección, monitoreo y respuesta ante incidentes para los Endpoints que cubren el alcance de la herramienta, cuenta con una interfaz gráfica de gráficos y tendencias que facilitan las labores de monitoreo por parte de analistas e ingenieros de seguridad. La solución está ampliamente extendida a sistemas Windows, Linux, OSX, sistemas de nube AWS y Azure, además de sistemas virtuales y contenedores como Docker.	✓
LimaCharlie	LimaCharlie es descrito como una Platform as a Service PaaS, la solución es un sistema en nube que se gestiona desde allí mismo, la instalación de agentes para monitoreo de los Endpoints y contar con funcionalidades adicionales requieren un pago para mantener la infraestructura gestionada. Este sistema no fue tomado como parte de análisis adicionales en este trabajo dado que existen restricciones y uso sin costo asociados para la implementación.	✗
Velociraptor	Es un proyecto y solución bastante similar a Google Rapid Response, teniendo como acceso también una interfaz gráfica vía web, cuenta con soporte para diversos sistemas operativos y la documentación también se ve bastante completa. Aunque esta plataforma puede ser interesante como parte de las pruebas a efectuarse en la siguiente étapa, no será incluída al ser escogido GRR y por las limitaciones en tiempo para el desarrollo de este trabajo en el tiempo planteado. Esta solución tecnológica y las demás que no pudieron ser revisadas a detalle son parte de una oportunidad futura de investigaciones que tome otros alcances usando como insumo este trabajo final.	✗

Tabla 1. Elección de sistemas EDR a profundizar e incluir e PoC

4.1 Arquitectura y diseño de estos EDR

4.1.1 GRR

Google Rapid Response GRR es un marco de trabajo completo enfocado en la conducción de procesos de respuesta a incidentes e investigación de manera remota[14]. Su objetivo principal se centra en apoyar investigaciones y labores forenses de una manera rápida y escalable que cubra conjuntos completos de Endpoints que se encuentren integrados y monitoreados por el sistema.

Su arquitectura a alto nivel consiste en dos partes, los clientes y el servidor de gestión.

[14] Nota: La investigación remota de Endpoints cobra vital importancia en un ambiente empresarial donde, por restricciones geográficas, o de otra naturaleza, el acceso físico a un sistema por parte de un profesional en respuesta a incidentes o informática forense puede tomar gastos de tiempo valioso que es solventado a través de acceso remoto a uno o grupos completos de equipos para efectuar actividades de contención y remediación de una emergencia o crisis a nivel de seguridad.

Componentes

Cliente GRR: Es desplegado a los sistemas que pueden ser sujetos de investigación o que pueden convertirse en parte de una investigación a demanda, es decir, una vez se cuenta con información de inteligencia que amerite una revisión en profundidad de manera remota, como puede ser una estación de trabajo, por ejemplo.

GRR dispone versiones cliente para Linux, OS X y sistemas Windows.

Cuenta con habilidades de análisis de memoria y reglas YARA.

Recoge información detallada de la CPU, memoria, entre otros factores del estado del equipo.

Servidor: Sistema donde se centraliza e integra varios componentes que hacen posible la operación de la herramienta, además de la interfaz gráfica web de usuario para ver los datos recibidos de los Endpoints y su procesamiento.

En detalle, integra los siguientes elementos:

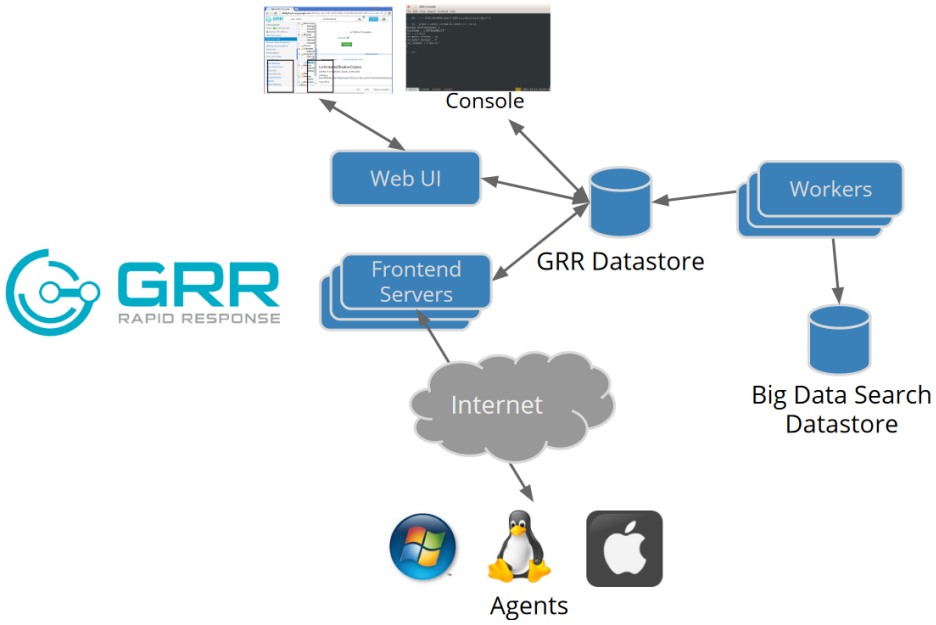


Ilustración 7. Arquitectura de GRR (Google Rapid Response). Tomado de https://storage.googleapis.com/docs.grr-response.com/ACSC%202015-%20Defending%20the%20Gibson%20in%202015.pdf

Datastore: El almacén de datos actúa como un componente de almacenamiento central para los datos y es un componente que orquesta la comunicación de todos los componentes del servidor GRR.

Frontend servers: Su función principal es descifrar las solicitudes POST de los clientes, desagrupar los mensajes contenidos y ponerlos en la cola de espera del Datastore.

Workers: Con el fin de eliminar tareas de procesamiento de datos, GRR implementó este componente. Los trabajadores verifican las colas del almacén

de datos para obtener respuestas del cliente, procesan nuevas solicitudes y flujos de comunicación.

Web UI: Aplicación central que permite al respondiente de incidentes o analista forense interactuar con GRR y facilita la conexión con la API de desarrollo, utilizada para labores de automatización e integración con otros sistemas.

4.2.1 Wazuh

Es un sistema y plataforma gratuita y de libre implementación de detección de amenazas, monitoreo de seguridad, respuesta a incidentes y cumplimiento regulatorio. Posee funcionalidades de monitoreo de Endpoints, servicios de nube y contenedores, y con posibilidades de uso y análisis de datos con la integración de herramientas externas. Wazuh proporciona las siguientes capacidades.

- Analítica de seguridad
- Detección de intrusos
- Análisis de logs
- Monitoreo de archivos ante cambios (Integridad)
- Detección de vulnerabilidades
- Repuesta a incidentes
- Monitoreo de entornos en nube
- Seguridad de contenedores (Docker)

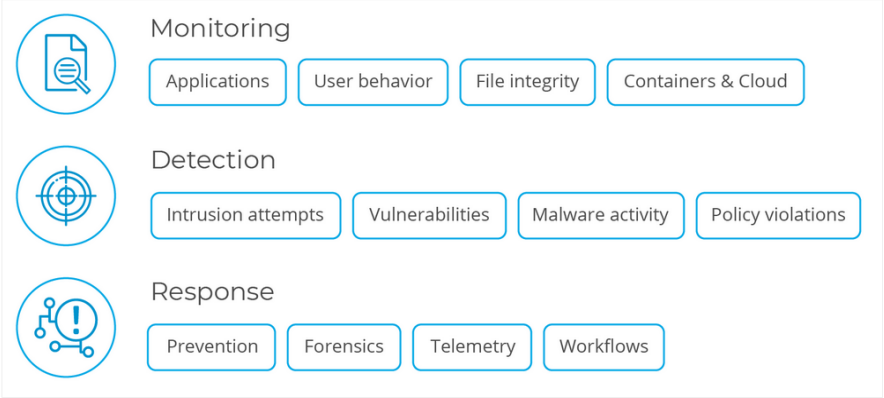


Ilustración 8. Características de Wazuh.
Tomado de https://documentation.wazuh.com/3.10/getting-started/index.html

Componentes

Sus grandes componentes principales son los agentes (O clientes), que reportan centralizadamente al servidor, y desde este se orquestan todas las funcionalidades de la herramienta.

Agente de Wazuh

El agente para instalación y monitoreo sobre los Endpoints funciona en Windows, Linux, Solaris, BSD y sistemas operativos Mac, pueden ser empleados en sistemas físicos, virtuales e instancias de nube.

Diversas actividades y procesos son desarrollados por los agentes para monitorear la integridad de archivos, inspeccionar en eventos y logs y analizar las configuraciones del sistema. A continuación, se presenta el diagrama relacionado al agente:

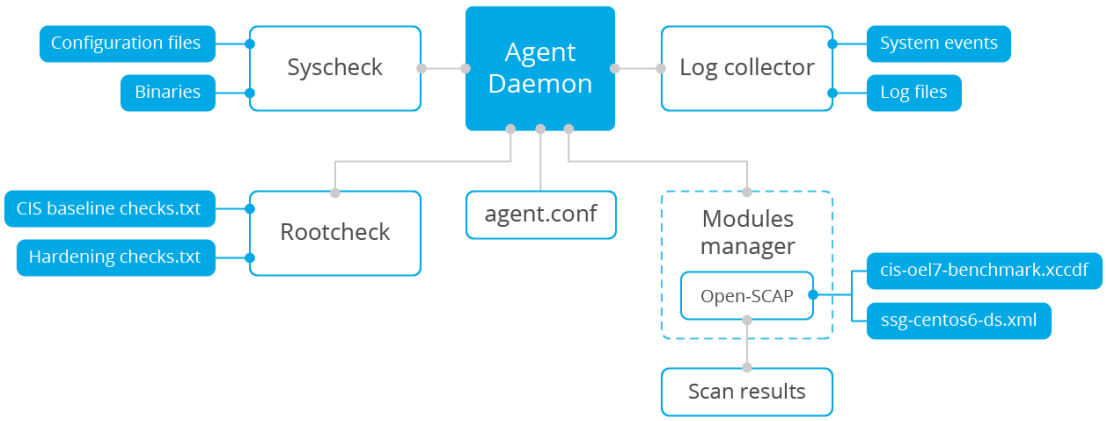


Ilustración 9. Estructura y componentes del cliente de Wazuh
Tomado de https://documentation.wazuh.com/3.10/getting-started/components.html#wazuh-agent

Rootcheck: Actividades relacionadas a detección de rootkits, malware y otras anomalías que pueden percibirse sobre el sistema.

Log Collector: Componente que lee logs del sistema y logs de aplicaciones, puede configurarse también para ejecutar y capturar datos periódicamente.

Syscheck: Monitoreo de integridad de los archivos, detecta cambios en el contenido de los archivos, así como la creación y borrado de archivos.

OpenSCAP: Utiliza líneas base de seguridad OVAL (Open Vulnerability Assessment Language) y XCCF (Extensible Configuration Checklist Description Format). Monitorea los sistemas apoyado en estos estándares para determinar aquellos que no están siguiendo configuraciones seguras.

Agent Daemon: Recibe los datos generados y recolectados por otros componentes del agente, los comprime, realiza un proceso de cifrado y los proporciona al servido a través de un canal seguro.

Servidor de Wazuh

Se encarga de analizar la información proveniente de los Endpoints facilitada por los agentes (O clientes) y generar alertas cuando un evento se correlaciona con una regla de seguridad, como una intrusión, un cambio sospechoso en un archivo, identificación de un rootkit, etc.

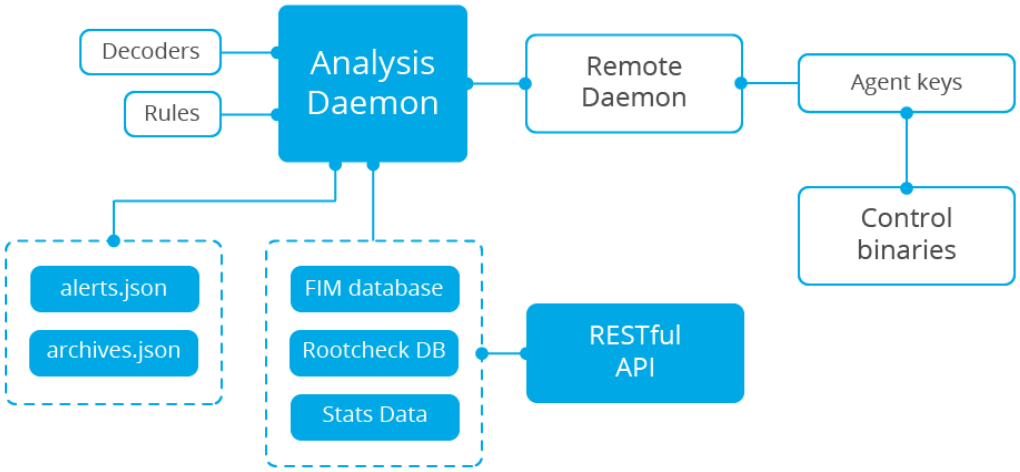


Ilustración 10. Estructura y componentes del servidor de Wazuh
Tomado de Tomado de https://documentation.wazuh.com/3.10/getting-started/components.html#wazuh-agent

El servidor por lo general se implementa en un único sistema físico, máquina virtual o sobre una instancia de nube, los principales componentes del servidor son:

Registration service: Usado para el registro de nuevos agentes a través del aprovisionamiento de llaves de autenticación que son únicas para cada agente.

Remote Daemon service: Recibe los datos de los agentes. Utiliza llaves de encripción para validar la identidad del agente y para cifrar las comunicaciones servidor – agente.

Analysis daemon: Realiza el análisis de datos. A través de decodificadores identifica el tipo de información que será procesada (como eventos de sistema, logs de servicio web, etc.) y realiza una extracción de los datos más relevantes en términos de seguridad de estas fuentes, como IPs, ID de eventos, entre otros que pueden determinar la activación de alertas y generar sugerencias de respuesta, como el bloqueo de una IP en infraestructuras perimetrales como firewalls u otros.

RESTful API: Proporciona una interfaz para gestionar y monitorear la configuración y observar el estado de los agentes, es usado también por la interfaz web de Wazuh, que es el sistema Kibana.

Elastic Stack

Es una suite open-source desarrollada para la administración de logs, incluye Elasticsearch, Kibana, Filebeat entre otros. Los componentes más relevantes para Wazuh son:

Elasticsearch: Un potente motor de análisis y búsqueda de texto.

Kibana: Una interfaz web para la visualización y análisis de datos.

Filebeat: Componente que envía logs a través de una red, generalmente para presentarlos a Elasticsearch.

Wazuh se integra con Elastic Stack para proporcionar una fuente de mensajes de registro ya decodificados para que Elasticsearch los indexe, así como una consola web en tiempo real para alertas y análisis de datos de registro. Además, la interfaz de usuario de Wazuh (que se ejecuta en la parte superior de Kibana) se puede usar para administrar y monitorear su infraestructura de Wazuh.

4.2 Definiciones de Hardware / Software para desarrollo de PoC

Analizando la documentación de los proyectos GRR y Wazuh, al tener elementos comunes en la manera de trabajo y su arquitectura cliente–servidor, el objetivo de la PoC es poder probar estos sistemas y sus capacidades frente a amenazas e infecciones reales sobre el monitoreo de un Endpoint.

El ajuste del ambiente para la ejecución del laboratorio se realizará en un equipo anfitrión con las siguientes características:

Sistema operativo: Windows 10 - 64 bits.

Procesador: Intel(R) Xeon(R) CPU E3-1505M v5 @ 2.80GHz 2.81 GHz

RAM: 64,0 GB

En cuanto al software empleado, se empleará VMware Workstation versión 14 con el fin de virtualizar los sistemas descritos en la Ilustración 11.

El diagrama a continuación proporciona un esquema a nivel gráfico de lo que se pretende realizar para la PoC, donde se infectará deliberadamente un cliente víctima Windows con una variante de malware y que se encuentre previamente registrada y monitoreada ante los servidores de GRR y Wazuh respectivamente. Las pruebas se realizarán de forma separada cuidando que se realicen en las mismas condiciones con el fin de observar las capacidades.

Ilustración 11. Esquema gráfico de componentes para PoC

5. Experimentación y desarrollo de PoC

5.1 Configuraciones del ambiente

5.1.1 Servidor GRR

El servidor GRR se implementó un sistema Ubuntu de 64 bits siguiendo la guía de configuración proporcionada por la documentación del proyecto en https://grr-doc.readthedocs.io/en/latest/installing-grr-server/from-release-deb.html

GRR se soporta sobre una base de datos MySQL como backend y es necesaria para el funcionamiento correcto del servidor, esta configuración se podría realizar sobre la misma infraestructura física o en un sistema independiente dependiendo de la arquitectura, diseño e implementaciones a nivel empresarial que requieren sistemas dedicados y alto procesamiento. Para esta PoC se realizarán las configuraciones sobre un único sistema.

A continuación, se presenta con un nivel de detalle moderado los pasos necesarios para la creación y construcción del ambiente, éstos deben ser ejecutados con privilegios administrativos.

Instalación de la base de datos:

```
apt install -y mysql-server
```

Se lanzará una ventana directamente en la shell de comandos solicitando la contraseña del usuario ‘root’ de la base de datos, el proceso continúa como se detalla en los demás comandos de configuración.

`mysql -u root -p` Solicitará la contraseña del usuario root (la que fue asignada previamente).

```
mysql> SET GLOBAL max_allowed_packet=41943040;
```

```
mysql> CREATE USER 'grr'@'localhost' IDENTIFIED BY 'password';
```

```
mysql> CREATE DATABASE grr;
```

```
mysql> GRANT ALL ON grr.* TO 'grr'@'localhost';
```

Se debe tener en cuenta que el valor max_allowed_packet no debe ser inferior a 20971520. La creación de un usuario adicional es opcional ya que es posible usar las credenciales del usuario root para operar la base de datos, sin embargo, las buenas prácticas de seguridad lo recomiendan para evitar el uso en todo sistema de cuentas de “super administrador” o que poseen todos los privilegios administrativos habilitados.

Se descarga la última versión deb de GRR a la actualidad.

```
wget https://github.com/google/grr/releases/tag/v3.3.0.8
```

Se instala el servidor y sus dependencias.

```
sudo apt install -y ./grr-server_3.3.0-8_amd64.deb
```

Una vez se encuentre instalado, grr-server debería estar disponible y activo con el comando `systemctl status grr-server` recibiendo un mensaje similar al siguiente:

Ilustración 12. Verificación del estado del servidor GRR

Una vez instalado el servidor y al acceder a su interfaz gráfica vía web con la IP del servidor y una dirección en esta forma `http://GRR_IP_ADDRESS:8000`

5.1.2 Servidor Wazuh

El proyecto provee una máquina virtual basada en 64 bits con fines de testeo y para conocer el funcionamiento del sistema, posee las siguientes características:

- CentOS 7
- Wazuh 3.10.2
- Wazuh API 3.10.2
- Elasticsearch 7.3.2
- Filebeat 7.3.2
- Kibana 7.3.2
- Wazuh app 3.10.2-7.3.2

El acceso a esta máquina virtual una vez se encuentra encendida tiene las credenciales “root/wazuh”.

Configuraciones adicionales fueron realizadas en el archivo local_rules.xml en la siguiente ruta del servidor

```
/var/ossec/etc/rules/local_rules.xml
```

El archivo reemplazado en esta ruta corresponde a una serie de reglas que contribuyen a la mejora en la detección de Wazuh que son de uso libre en el recurso de GitHub https://github.com/sametsazak/sysmon. Estas reglas de detección pertenecen a la herramienta Sysmon, el cual será configurado en el siguiente apartado de construcción de la máquina víctima.

El acceso a Wazuh a su consola gráfica y de gestión se realiza a través de un navegador web en `https://DIRECCION_IP_WAZUH`, donde el valor de la IP corresponde a la dirección del servidor y se obtiene a través del comando `ip addr` en CentOS, sistema operativo donde se encuentra Wazuh en la máquina virtual ofrecida para pruebas por sus desarrolladores.

Por otra parte, es posible configurar localmente elementos adicionales para cada Endpoint en el archivo *ossec.conf* que se crea como parte del sistema de archivos del agente, allí es posible incluir la lectura del log de Sysmon dado que no es una funcionalidad de Wazuh por defecto. Lo anterior puede ser replicado de dicha manera a gran escala al interior de una organización, sin embargo, la mejor opción puede hacerse de manera centralizada en el servidor de Wazuh a través del archivo *agent.conf* en la ruta `/var/ossec/etc/shared/default`. La información que se incluya en el archivo será parte de información complementaría recolección de logs para Wazuh. La imagen a continuación ilustra la edición de éste para la PoC incluyendo Sysmon, eventos del Antivirus Windows Defender que viene por defecto en sistemas Windows, y actividad de comandos WMI que actualmente es muy usada por amenazas recientes.

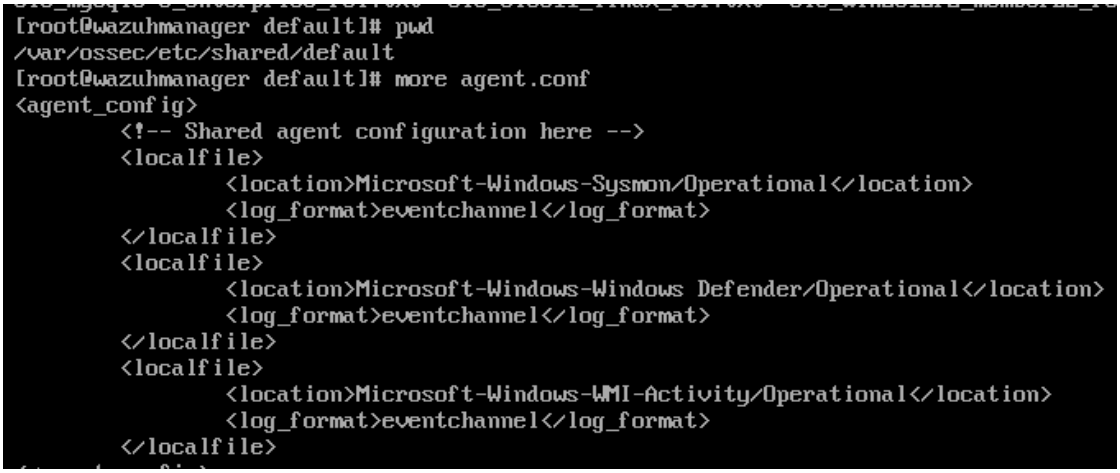


Ilustración 13. Configuración centralitzada monitoreo logs cliente en Wazuh

5.1.3 Equipo victima Windows 10

Con el fin de emular un equipo que puede ser parte de un ambiente tecnológico empresarial, se empleó una versión Windows 10 Enterprise de 64 bits. Este tipo de sistemas son de uso común por roles administrativos y otros que realizan labores de análisis, uso de Microsoft Office y correo electrónico.

Este sistema fue instalado sin ninguna configuración o software especial adicional a excepción de Microsoft Office 365 y la herramienta System Monitor (Sysmon)[15] de la suite Sysinternals Tools. Esta última fue desarrollada de manera especial por Microsoft para obtener mayor trazabilidad sobre las

[15] https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

acciones del sistema como la ejecución de programas, conexiones de red a nivel de IP y dominios, además de contar con logs de acciones realizadas en línea de comandos; llegar a identificar su implementación en ambientes de empresa es un beneficio para los roles de respuesta a incidentes, analistas forenses y que desempeñan funciones de caza de amenazas, considerándose un artefacto forense de alto valor que proporciona inteligencia accionable durante la investigación por un incidente de seguridad; desafortunadamente no es una función predeterminada de sistemas Windows.

Sysmon puede ser instalado en forma estándar o con un archivo de configuración que refine y acote los eventos registrados, se instaló sobre el sistema Windows con el archivo sysmonconfig-export.xml que es de libre uso en el repositorio GitHub https://github.com/SwiftOnSecurity/sysmon-config con la siguiente línea de comando:

```
Sysmon64.exe -accepteula -i sysmonconfig-export.xml
```

Sysmon cuenta con versiones de 32 y 64 bits, el comando anterior representa la instalación en su versión de 64 bits, que fue empleada en la ejecución de pruebas del presente trabajo.

La instalación de Sysmon consiste en la creación de un log adicional parte del visor de eventos de Microsoft, el archivo *Microsoft-Windows-Sysmon/Operational*. El log cuenta con trazabilidad de los siguientes eventos:

Category	Event ID
Process Create	1
Process Terminated	5
Driver Loaded	6
Image Loaded	7
File Creation Time Changed	2
Network Connection	3
CreateRemoteThread	8
RawAccessRead*	9
Sysmon Service State Change	4
Error	255

Ilustración 14. Eventos capturados por Sysmon
Tomado de https://onedrive.live.com/view.aspx?resid=D026B4699190F1E6!2575&ithint=file%2cpptx&authkey=!AGFBok7JLkOZSgE

5.2 Emotet - Muestra de malware seleccionada

En la actualidad, una de las categorías más grandes de malware que han constituido casos mediáticos presentados en Internet, televisión, redes sociales y otros medios de difusión a nivel mundial por su impacto y pérdidas económicas asumidas por diferentes tipos de organizaciones, corresponden a

familias de ransomware, que es una vertiente de software malicioso que ataca el contenido de archivos sobre un sistema de cómputo aplicando algoritmos de criptografía que cifran los ficheros e impiden su visualización y uso solo hasta ser desbloqueados con una llave (O contraseña) para su descifrado. La amenaza cibernética crea un mensaje con instrucciones puntuales al usuario final para efectuar un pago para recibir del atacante la llave, asociándose a una forma rescate por la recuperación de los archivos y su información almacenada. La amenaza más representativa en este aspecto fue la conocida como Wannacry en 2017, que afectó a Telefónica[16], siendo quizás el ataque cibernético más famoso de la actualidad, tras las operaciones del grupo Carbanak[17] del año 2014.

Al desarrollo de esta investigación (Noviembre 2019) recientemente se han conocido casos mediáticos y de impacto considerable por ransomware puntualmente en España y México en las compañías Everis, la cadena de radio SER y Petróleos Mexicanos (PEMEX).

Ilustración 15. Datos sobre el ataque efectuado a Everis
Tomado de Twitter - https://twitter.com/ProtAAPP/status/1192064195597963265

Estos casos en Europa y América Latina relacionados al malware Emotet, desplegaron amenazas de ransomware Bitpaymer[18] y DopplePaymer[19] en los casos de España y México respectivamente.

[16] https://www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/
[17] https://www.kaspersky.com/blog/billion-dollar-apt-carbanak/7519/
[18] Mayor detalle acerca del ataque en https://www.virustotal.com/gui/user/PussyLover/comments
[19] https://www.excelsior.com.mx/nacional/exigen-a-pemex-49-millones-de-dolares-ciberdelincuentes-demandan-pago/1347395

5.2.1 Algunos datos sobre Emotet

Es un software malicioso categorizado como troyano, correspondía a un malware bancario que fue identificado por primera vez hacía el año 2014, sus objetivos iniciales consistían en el robo de información. Al malware se han añadido nuevas funcionalidades que lo potencian y lo hacen aún más peligroso infectando organizaciones con redes de equipos y tecnología a gran escala, su propagación puede darse a través de campañas de phishing a buzones de correo sin ningún criterio especial, o dirigido con el fin de atacar un grupo o empresa puntual, técnica conocida como spear-phishing.

Ataques más sofisticados efectuados por atacantes para infectar con Emotet diferentes a Phishing, son aquellos conocidos como “drive by download”, que implica la ejecución del malware por acción humana de la víctima con la excusa de visualizar todo o parte del contenido de un sitio web comprometido, o efectuar una actualización al navegador, permitiéndose la instalación del código malicioso en el sistema sin ser percibido por la víctima.

Con el fin de realizar la PoC, se ha escogido esta amenaza puntual con el fin de infectar deliberadamente el sistema configurado como víctima. La variante de Emotet en este caso se encuentra al interior de un documento Microsoft Word (.doc). Microsoft por protección del usuario luego de identificar que actores maliciosos desarrollaban código en estos documentos, decidió restringir la ejecución de macros de manera predeterminada, para que la amenaza se ejecute, es necesario dar clic y aceptar el acuerdo de licencia… Como bien lo sugiere el atacante al diseñar el archivo.

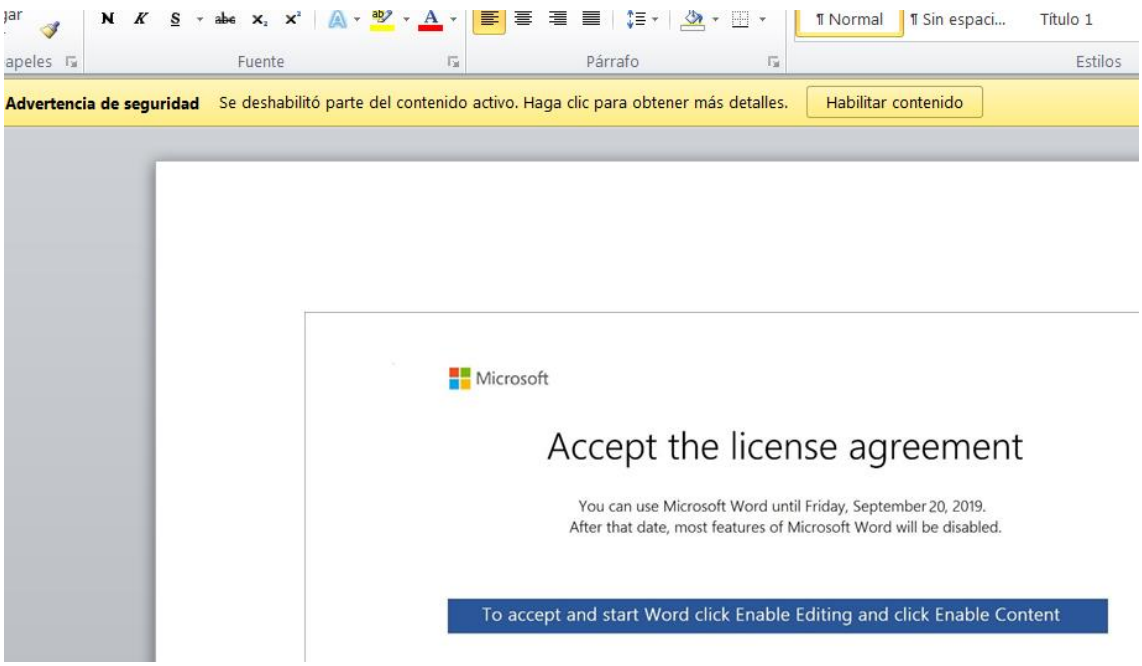


Ilustración 16. Archivo malicioso con Emotet en su contenido

Muestra emotet	Nombre: emotet.doc Cambiado a citación.doc con motivos de esta prueba
Valores hash	MD5: B92021CA10AED3046FC3BE5AC1C2A094. SHA1: 0FB1AD5B53CDD09A7268C823EC796A6E623F086F SHA256: C378387344E0A552DC065DE6BFA607FD26E0B5C569751C79FBF9C6F2E91C9807
Mayor información	https://app.any.run/tasks/3363fde4-111b-4aaa-b73d-e4144433c284/

Tabla 2. Información relevante malware Emotet

5.3 Ejecución de amenaza y resultados EDR

La PoC desarrollada consiste en la ejecución del malware Emotet sobre el sistema víctima, el cual se encuentra bajo monitoreo previo mediante la instalación de agentes cliente con el fin de obtener la visibilidad del Endpoint correspondiente en las consolas gráficas de los servidores GRR y Wazh implementadas. Estas pruebas se realizarán de manera separada y con monitoreo independiente de la máquina víctima, empleando instantáneas o snapshots del sistema para garantizar que el monitoreo se realiza en las mismas condiciones en cada caso.

5.3.1 Experimentación con GRR

Una vez instalado el servidor y al acceder a su interfaz gráfica vía web con la IP del servidor y una dirección en esta forma `http://GRR_IP_ADDRESS:8000` desde un navegador web, podemos obtener los agentes de instalación para despliegue de los clientes:

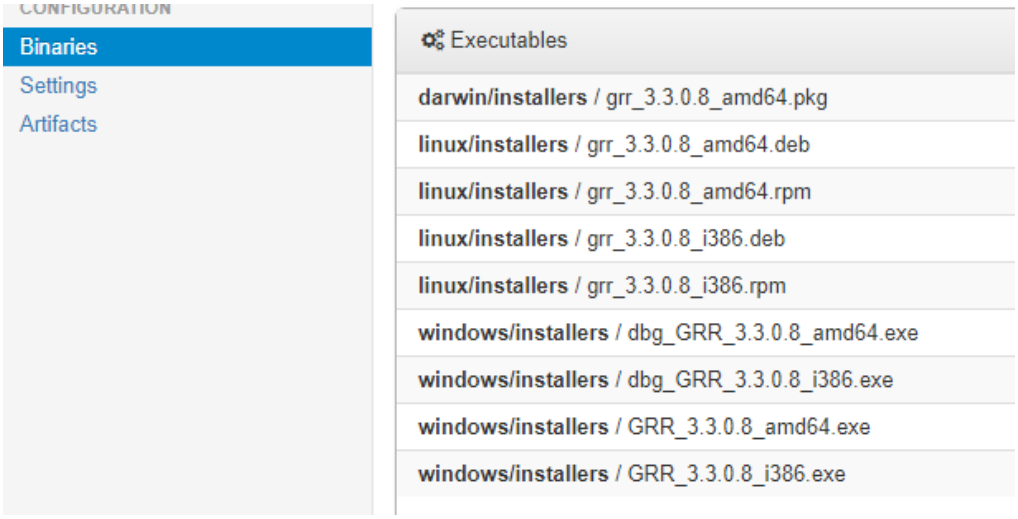


Ilustración 17. Agentes de instalación disponibles desde el servidor GRR

El agente se puede instalar de manera remota a través de herramientas como psexec u otros medios para implementación a escala como reglas de Directorio

Activo entre otros, en la consola de GRR se reportarán los clientes para obtener visibilidad del Endpoint a través del servidor.

Online	Subject	Host	OS Version	MAC	Usernames	First Seen	Client version
	C.90fec499577799a5	Noriben-PC.localdomain	6.1.7600SP0	00:0c:29:27:da:51 94:39:e5:aa:e9:92	Noriben	2019-11-24 21:54:10 UTC	3308

Ilustración 18. Equipo víctima de la PoC monitoreado por GRR

GRR tiene un código de colores en el cual se puede identificar el estado de de los clientes conectados a él, en verde se detalla estado activo o encendido del equipo remoto, si estuviera inactivo, el color cambia a amarillo, y finalmente en rojo si no se percibe comunicación con el agente o el endpoint monitoreado se encuentra apagado.

La amenaza de malware ejecutada se realizó desde la localización de descargas del equipo víctima, simulando un caso común de phishing donde el usuario descarga el archivo y busca observar su contenido. El nombre del archivo es citacion.doc, que puede correspoder a un escenario en el que se engaña a la víctima provocando una sensación de urgencia en algún aspecto.

Desde GRR es posible detectar esta amenaza mediante una búsqueda de archivos a través de la ejecución de un nuevo flujo con la opción “Start New Flows” en el menú izquierdo de opciones de GRR.

A través de la opción File Finder, es posible realizar una búsqueda sobre el Endpoint del archivo malicioso con el fin de confirmar rápidamente un posible compromiso del equipo e incluso recolectar el archivo remotamente con fines de análisis. En el caso que se observará a continuación, se realizó una búsqueda puntual del nombre del archivo (citación.doc), no obstante, es posible efectuar una búsqueda de ficheros con esta extensión de la forma **.doc.

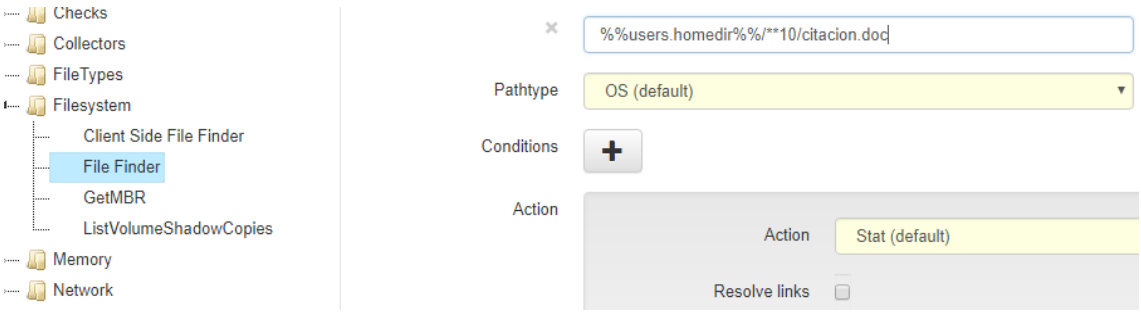


Ilustración 19. Búsqueda de archivo sospechoso

El comando anterior %%users.homedir%%**10\citacion.doc corresponde a una búsqueda alrededor de todos los usuarios de sistema, y con una profundidad de 10 directorios adicionales (**10), realiza inspección de un archivo denominado citacion.doc. Los resultados de la ejecución de este flujo se observan a continuación.

Launched Flow FileFinder:

Urn	aff4:/C.c80a15f87edc77ba/5B65EBE4			
Flow id	5B65EBE4			
Client id	C.c80a15f87edc77ba			
Name	FileFinder			
Args	Paths	%%users.homedir%%/**10/citacion.doc		
	Action	Action	STAT	
		Stat	Collect extended attributes	false
Runner args	Notify at Completion	true		
	Client id	C.c80a15f87edc77ba		
	Flow name	FileFinder		
State	RUNNING			
Started at	2019-11-25 02:22:24 UTC			
Last active at	2019-11-25 02:22:24 UTC			
Creator	admin			

Ilustración 20. Información de flujo y búsqueda ejecutada

Información mas detallada puede observarse en la opción “Managed launched flows” de GRR, donde se condensa entre los resultados la información correspondiente a la ruta completa en la cual se encuentra el archivo en la carpeta de Descargas del usuario Noriben (C:\Users\Noriben) en la parte inferior de la imagen a continuación.

Value			
Payload	Stat entry	Aff4path	aff4:/C.c80a15f87edc77ba/fs/os/C:/Users/Noriben/Downloads/citacion.doc
		St mode	-rw-rw-rw-
		St ino	0
		St dev	0
		St nlink	0
		St uid	0
		St gid	0
		St size	143202
		St atime	2019-11-18 12:08:52 UTC
		St mtime	2019-11-18 12:08:52 UTC
		St ctime	2019-11-18 12:08:52 UTC
		St flags osx	
		St flags linux	----------
		Pathspec	Pathtype OS
			Path /C:/Users/Noriben/Downloads/citacion.doc

Ilustración 21. Resultados e identificación puntual de archivo sospechoso

En la parte superior de la imagen encuentra un link o hipervinculo con el cual GRR presenta el archivo en la ruta en la cual fue identificado a través del árbol de archivos del sistema, donde se puede obtener remotamente la muestra o incluso observar sus valores hash con el fin de confirmar la posibilidad de compromiso sobre este host.

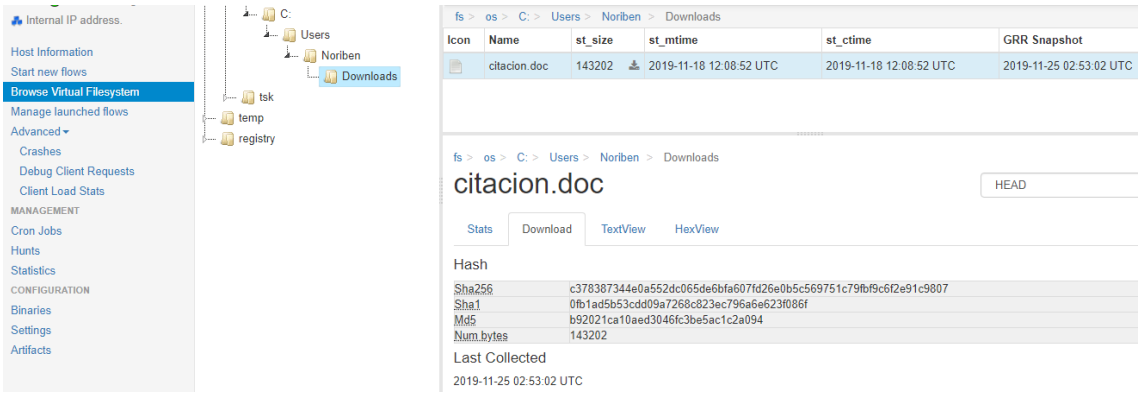


Ilustración 22. Árbol de archivos y valores hash del archivo sospechoso

La verificación de este valor hash, fue inspeccionado en VirusTotal, que es una fuente adicional de inteligencia que puede ser usada con la información recolectada con GRR.

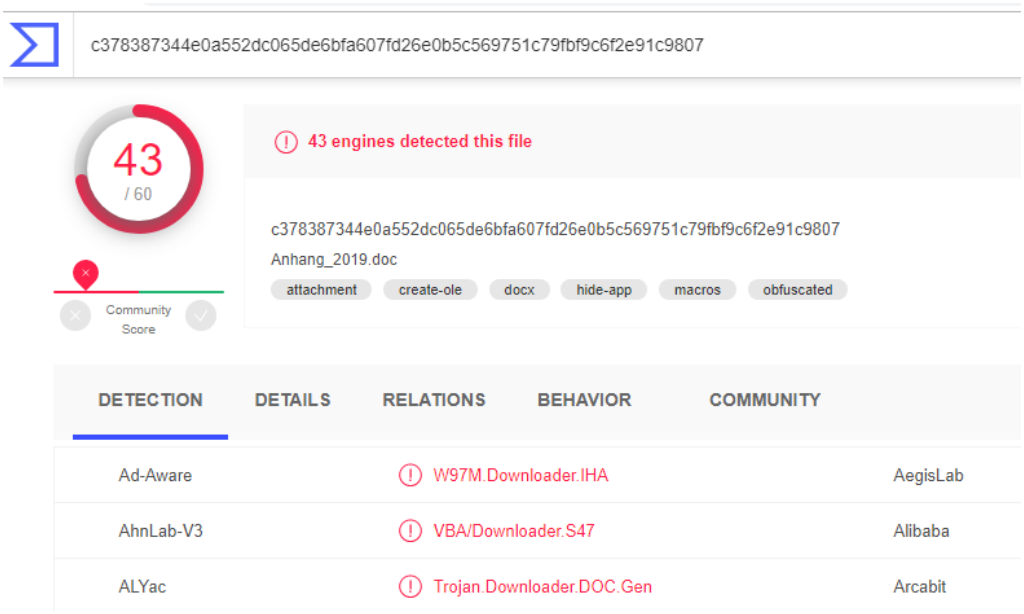


Ilustración 23. Confirmación que el archivo corresponde a malware

GRR puede ser utilizado para inspeccionar también el registro de Windows y revisar llaves puntuales que son creadas de manera común por malware para crear persistencia y mantener el endpoint comprometido incluso si este es reiniciado, por otra parte puede recoger logs y otros artefactos del sistema que proporcionan un análisis como parte del incidente y de informática forense.

La recolección de logs del visor de eventos es una de las funcionalidades de GRR, como ejemplo se realizó la búsqueda del log de Sysmon y se descargó para análisis adicionales con otras herramientas o a través del visor de eventos proporcionado de manera nativa por los sistemas Microsoft Windows.

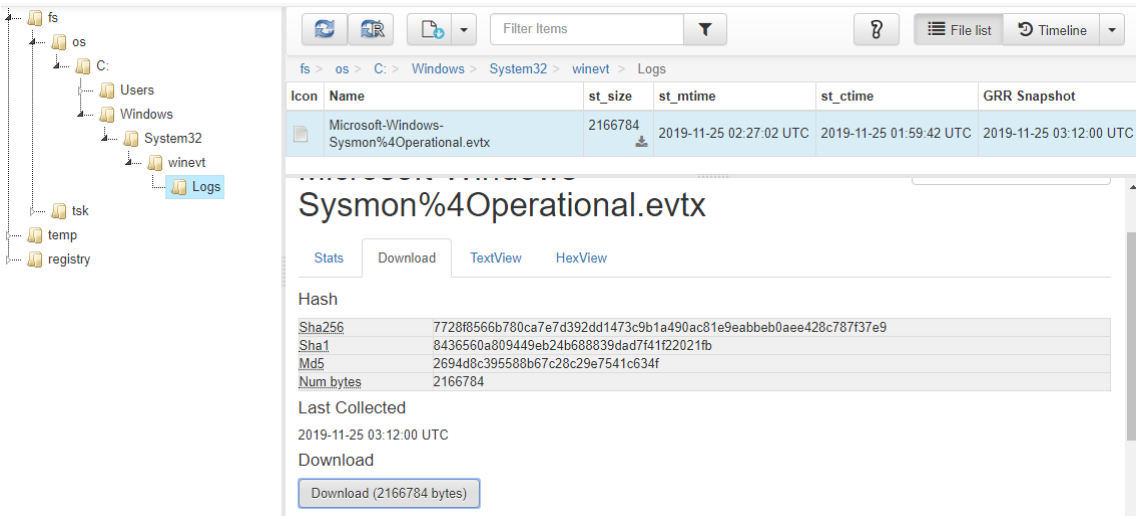


Ilustración 24. Búsqueda y recolección del log Sysmon del sistema

Un análisis de este log presenta la apertura del archivo por parte de Microsoft Word.

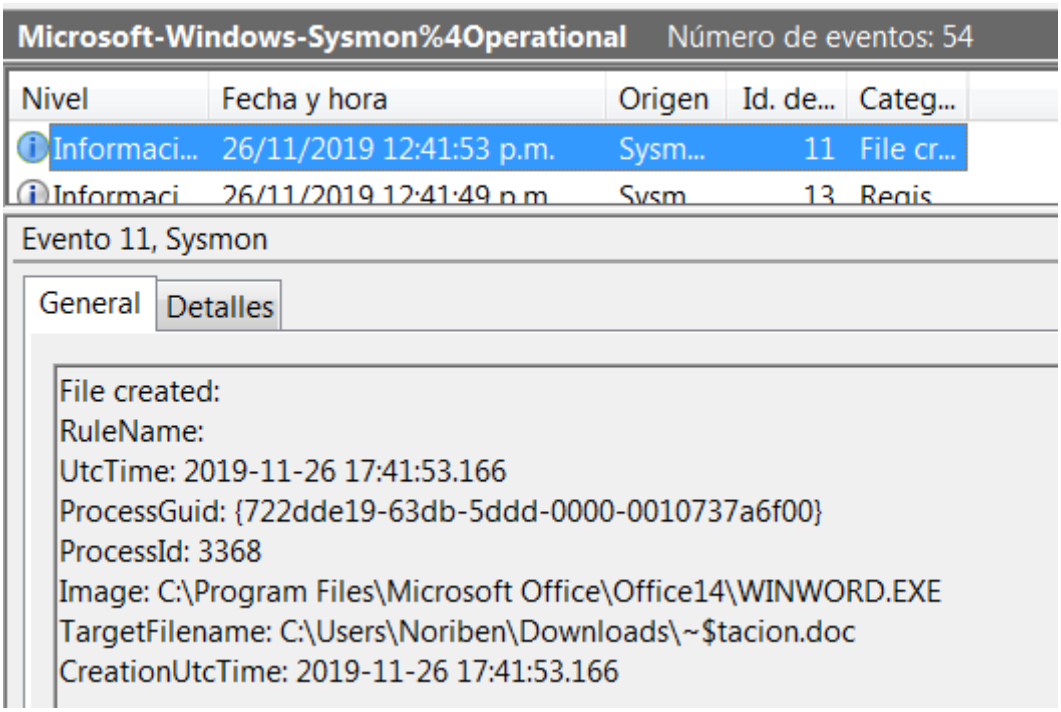


Ilustración 25. Hallazgo de archivo de malware abierto por MS Word

Y más adelante, es posible observar la ejecución de un comando codificado a través de Powershell

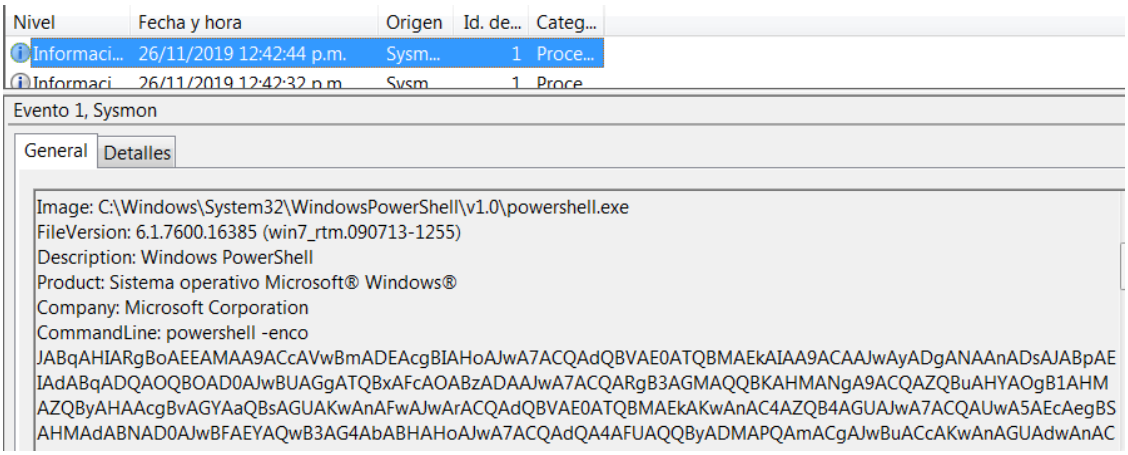


Ilustración 26. Ejecución de código en Powershell

Lo anterior, corresponde a un código codificado en Base64, comunmente usado por diferentes variantes maliciosas que ejecutan comandos sobre sistemas con el fin de completar sus diferentes objetivos, como robo de información, comprometer otros sistemas, hacer equipos parte de una botnet, o cifrarlos para extorsionar usuarios o empresas solicitando un rescate para recuperar información afectada. Para visualizar el código de en un nivel de abstracción más fácil al entendimiento humano, se usa una herramienta de conversión entre formatos, este es un ejemplo del servicio CyberChef (https://gchq.github.io/CyberChef/). A través de estos hallazgos es posible obtener información adicional de inteligencia respecto a la amenaza, y obtener indicadores de compromiso adicionales como direcciones IP y dominios de Internet, los cuales deberían ser usados para tomar acciones de tipo proactivo e incluirlas en listas restrictivas y con el fin de identificar el alcance completo de la amenaza sobre la red, para efectuar una mitigación y erradicación de este posible incidente por el malware Emotet.

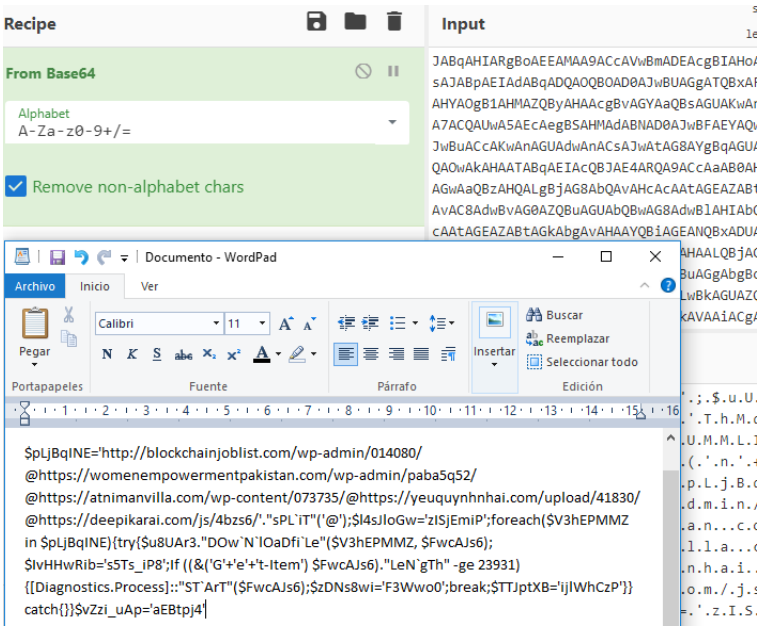


Ilustración 27. Conversión Powershell Base64 hallada con GRR

5.3.2 Experimentación con Wazuh

Una vez el servidor Wazuh se encuentra en funcionamiento, se puede proceder al despliegue de los agentes, los binarios son proporcionados por los desarrolladores del proyecto en https://documentation.wazuh.com/3.10/installation-guide/packages-list/index.html#packages, allí es posible identificar los instaladores para todas las plataformas soportadas.

Luego de descargarse el archivo, es posible desplegar el binario a través de Directivas de Grupo GPO (Directorio Activo), Powershell a nivel remoto, comandos WMI o psexec al igual que puede darse el despliegue del agente de GRR en entornos empresariales donde se requieren implementaciones a gran escala. Una vez se encuentra alojado el archivo en el Endpoint, su instalación puede realizarse a través de la consola gráfica, lo cual requiere acción humana en cada sistema o realizarse a través de línea de comandos[20]:

En CMD:

```
wazuh-agent-3.10.2-1.msi /q ADDRESS="10.0.0.2" AUTHD_SERVER="10.0.0.2"
```

En Powershell:

```
.\wazuh-agent-3.10.2-1.msi /q ADDRESS="10.0.0.2" AUTHD_SERVER="10.0.0.2"
```

A través de estos comandos, se realizará la instalación y proceso de registro del agente para que sea identificado por Wazuh.

Accediendo mediante un navegador web en `https://DIRECCION_IP_WAZUH`, se visualizará la interfaz de Kibana, que es la ventana de acceso a ElasticStack y a través del cual se puede identificar Wazuh en el panel izquierdo a través de su logo. A continuación, se presenta el sistema víctima que se encuentra en monitoreo a través de la interfaz gráfica:

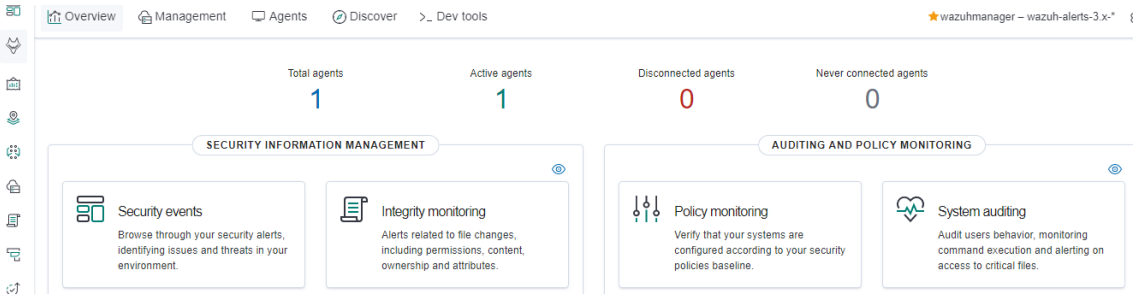


Ilustración 28. Panel principal de opciones Wazuh

En la opción “Agents” en la parte superior es posible identificar la información de los sistemas que están siendo monitoreados.

[20] Información para instalación del agente Wazuh en sistemas Windows https://documentation.wazuh.com/3.10/installation-guide/installing-wazuh-agent/windows/wazuh_agent_package_windYows.html

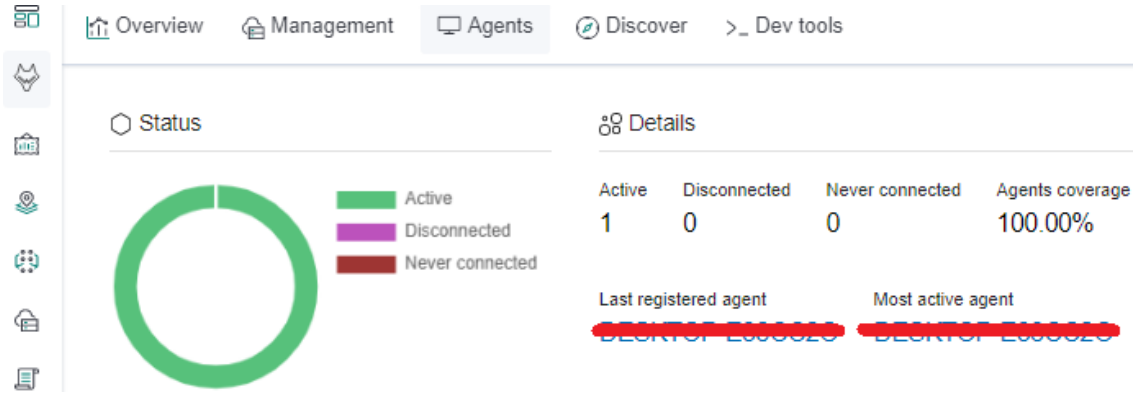


Ilustración 29. Visaualización de agentes monitoreados desde Wazuh

Los eventos de seguridad es una funcionalidad que presenta una serie de gráficas e información estadística, además de presentar las alertas relevantes. Con el sistema infectado por la infección de Emotet, se pueden observar eventos relacionados.

Alerts summary

Rule ID	Description	Level	Count
255016	Detects suspicious PowerShell invocation command parameters	12	1
255071	Detects a suspicious command line execution that includes an URL and AppData	12	2
62103	Windows Defender: detected potentially unwanted software C:\Windows\SysWOW64\cmd.exe	12	4
60776	SessionEnv was unavailable to handle a critical notification event	7	1
62104	Windows Defender: taken action to protect machine from unwanted software C:\Windows\SysWOW64\WMIScriptingAPI\nssy.exe	7	2
19007	Benchmark for Windows audit: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'	7	1
550	Integrity checksum changed.	7	41
61109	Name resolution for the name wpad timed out	5	1
554	File added to the system.	5	1

Ilustración 30. Alertas de seguridad detectados por la infección de Emotet

Aquellos eventos con cuyo prefijo es 255 están relacionadas con las alertas Sysmon que fueron configuradas previamente. Ya que Wazuh a nivel estándar monitorea en Windows los logs de eventos representativos Security, System y Application, puede hacerse más difícil la detección de malware, este tema será tratado dentro de las conclusiones y trabajo futuro de este trabajo.

Para el caso de la muestra de malware usada en esta PoC, el evento más representativo se percibe en la ejecución de Powershell con comandos sospechosos (Detects suspicious PowerShell invocation command parameters), al revisar a detalle la alerta a través de la opción “Discover” de Wazuh es posible obtener trazabilidad completa del comando ejecutado sobre el sistema víctima.

Ilustración 31. Información de evento detallada sobre equipo afectado

El comando identificado al ser traducido en la codificación Base64 como viene originalmente, puede proporcionar información de inteligencia accionable que lleve a acciones de contención en herramientas de seguridad a través del bloqueo de datos de conexión a servidores de comando y control (C2) u otros.

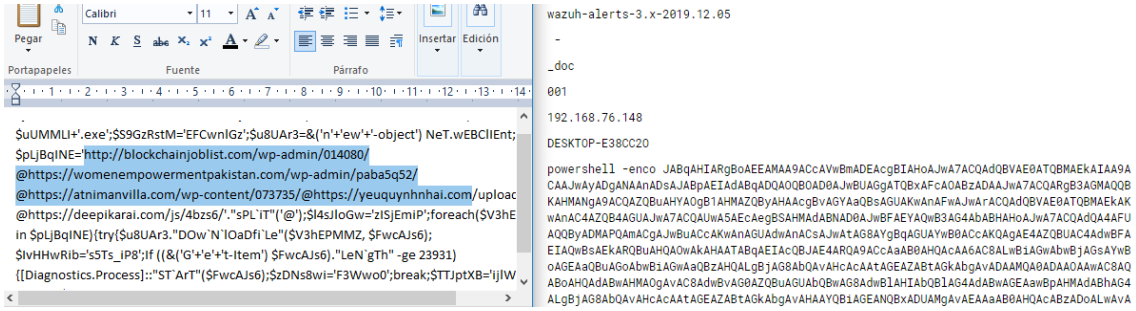


Ilustración 32. Conversión Powershell Base64 hallada con Wazuh

6. Análisis de resultados

6.1 Análisis de características Gartner en EDRs testeados

Luego de experimentación con los sistemas GRR y Wazuh a través de su implementación realizando una PoC y observando las funcionalidades frente a la infección deliberada de un equipo monitoreado por estas soluciones de seguridad, a continuación, se presentan las conclusiones obtenidas de las pruebas efectuadas y la satisfacción de requisitos que cumplen en relación con las cuatro características enunciadas por Gartner para un sistema EDR, se debe tener en cuenta que la naturaleza de cada uno de estos sistemas no fue diseñada partiendo de estos principios y sus desarrolladores no estaban creando un sistema EDR, no obstante a lo anterior, como se verá en las conclusiones, es posible cubrir estas características con algunos límites.

Característica - Habilidad de detectar incidentes de seguridad cuando ocurren	
GRR	Aunque GRR no percibe en sus funcionalidades un monitoreo por defecto de archivos y la integración nativa de elementos de inteligencia como IoC, nombres de archivos sospechosos, listas maliciosas de IP/Dominios, entre otros que puedan generar alertas automatizadas respecto a la actividad de los Endpoint, esto se puede configurar a nivel manual a través de la programación de Hunts, dado que un sistema EDR es usado comúnmente para procesos de caza de amenazas (Threat hunting), GRR satisface estas necesidades. No obstante, es requerida acción y análisis humano para determinar anomalías relacionadas a compromisos en los Endpoint.
Wazuh	Wazuh cuenta con configuración de alertas y reglas de monitoreo sobre logs e integración de herramientas adicionales como VirusTotal, posee por defecto reglas que se activan y visualizan en la interfaz gráfica relacionadas a problemas de seguridad en los diferentes Endpoint Windows, Mac OSX y diversas variantes de Linux en las que se ofrece agente. Como se pudo observar en las pruebas efectuadas, es extensible a la recolección y análisis de logs adicionales además de creación de reglas personalizadas que pueden ser usadas para aplicativos y software propio de negocio. En general Wazuh se percibe como una herramienta que satisface bastante bien esta primera característica de detección a nivel de seguridad de un Endpoint, no obstante, requiere del establecimiento de reglas muy bien configuradas que permitan obtener información de calidad y que permita toma de decisiones.
Característica - Contener el incidente en el/los Endpoint(s)	
GRR	Dado que GRR fue diseñado principalmente con fines de investigación y recolección de datos a gran escala, sus funcionalidades tienen límites para efectuar acciones que contengan incidentes directamente sobre los Endpoint, no obstante, la información identificada en GRR puede ser de valía a través del uso de software adicional que pueda contener procesos maliciosos, inclusión de reglas de Antivirus, listas negras y/o reglas de control en Firewalls y de navegación. Adicionalmente, GRR cuenta con una API con la cual se pueden crear interfaces o conexiones con otras tecnologías que habiliten estas actividades.
Wazuh	Provee una funcionalidad denominada Active Response, que es un conjunto de contramedidas para abordar las amenazas detectadas, al igual que las reglas, estas acciones son ejecutadas cuando se cumplen ciertos criterios. Las respuestas activas son similares a las reglas de monitoreo configurándose también en XML y que al activarse ejecutan un script de respuesta. Wazuh provee una serie de scripts preconfigurados en Windows y Linux como parte de su documentación[21]. Esta funcionalidad debe ser usada con cuidado ya que implementaciones débiles de reglas pueden dar lugar a errores o aumentar las vulnerabilidades del sistema.

[21] https://documentation.wazuh.com/3.10/user-manual/capabilities/active-response/how-it-works.html#default-active-response-scripts

	Muchas actividades de contención-remediación pueden ser sensibles respecto al impacto en disponibilidad o errores en tecnología ya que deben realizarse de manera directa en ambientes productivos, acciones representativas como remoción de archivos, parada de servicios, entre otros, deberían ser implementadas con intervención y control humano para que se garantice supervisión durante los procesos.
Característica - Soportar la investigación del incidente	
GRR	El cumplimiento de esta característica mencionada por Gartner en GRR puede satisfacerse bastante bien, ya que GRR provee sobre uno o grupos de Endpoints, la posibilidad de recolección de información que permita confirmar compromisos de seguridad sobre los Endpoint,
Wazuh	Da la posibilidad de obtener mayores datos a través de la revisión adicional de eventos en los logs monitoreados, Wazuh puede ser configurado para recoger todos los datos relacionados a los Endpoint en lugar de recolectar eventos específicos habilitando esta funcionalidad en el archivo ossec.conf del servidor. Esta información puede ser usada para tomar acciones de contención-erradicación a través de otros sistemas de seguridad complementarios. Adicionalmente, Wazuh tiene implementadas entre sus funcionalidades un motor de inspección que revisa la integridad y alerta respecto a cambios en el sistema, que incluye por ejemplo elementos sobre el registro de Windows donde pueden crearse o modificarse valores fruto de amenazas cibernéticas.
Característica - Proporcionar mecanismos para remediar la situación sobre el/los Endpoint(s) afectados	
GRR	Esta funcionalidad está muy relacionada con las características de contención enunciadas por Gartner, en GRR, se cuenta principalmente con opciones que permiten obtener la información suficiente que habilite procesos de remediación, sin embargo este no es un sistema que cuente con funcionalidades para limpiar sistemas, o deliberadamente restringir o eliminar la ejecución de archivos maliciosos, cambios o remociones de llaves de registro, entre otros elementos que pueden ser parte de un ataque al/los Endpoint.
Wazuh	Parte de esta funcionalidad puede llegar a satisfacerse a través de las funcionalidades de Active Response, sin embargo, estos procesos podrían representar riesgos en caso en que puedan dispararse reglas que puedan representar falsos positivos relacionados. La utilización de esta funcionalidad de respuesta requeriría de un diseño e implementación de las reglas además de la realización de pruebas frente a su adecuado funcionamiento.

Tabla 3. Conclusiones para GRR y Wazuh en relación con características de un EDR según Gartner

Con el ánimo de proporcionar una visión adicional de las conclusiones obtenidas, se esquematizó una escala y un diagrama que muestra los resultados a nivel gráfico, de las funcionalidades percibidas a través de la experimentación efectuada frente a las características definidas por Gartner para un sistema EDR, estos no se plasman para ser interpretados como una comparación entre GRR y Wazuh, se realiza con el fin de evidenciar los grados de suficiencia percibidos fruto del desarrollo de este trabajo, los cuales reflejan oportunidades de desarrollo y mejora con miras a la implementación práctica en ambientes productivos de una organización, y sea parte de adopciones estratégicas en la postura de seguridad teniendo en cuenta la funcionalidad, alcance y limitaciones de estas soluciones.

6.2 Escala propuesta de medición y evaluación de características Gartner

La ponderación registrada en la tabla de evaluación de estos sistemas corresponde con los resultados de la PoC y las justificaciones que fueron expresadas a nivel cualitativo, para cada uno de los componentes que debe cubrir una tecnología EDR según Gartner.

Niveles de adaptación a las características EDR Gartner	
Nivel	**Características**
1 - No suficiente	No cubre la característica en ninguna de sus funcionalidades o diseño por defecto. Requiere de un trabajo de diseño y construcción de software para lograr la funcionalidad
2 - Suficiente requiriendo mejoras	Cubre la característica Gartner requiriendo algunas mejoras en personalización de elementos, integración y creación de interfaces con otras tecnologías para cubrir la característica.
3 - Optimizado	Por defecto satisface adecuadamente la característica Gartner al tener una empatía fuertemente relacionada entre el propósito de diseño de la solución y la característica Gartner del EDR.

Tabla 4. Tabla de niveles de adaptación a las características EDR en relación con Gartner

Evaluación de funcionalidades de las soluciones en la PoC		
Característica	**GRR**	**Wazuh**
Habilidad de detectar incidentes	2	2
Contener el incidente	1	2
Soportar la investigación	3	2
Proporcionar mecanismos para remediación	1	2

Tabla 5. Evaluación de funcionalidades de las soluciones en la PoC

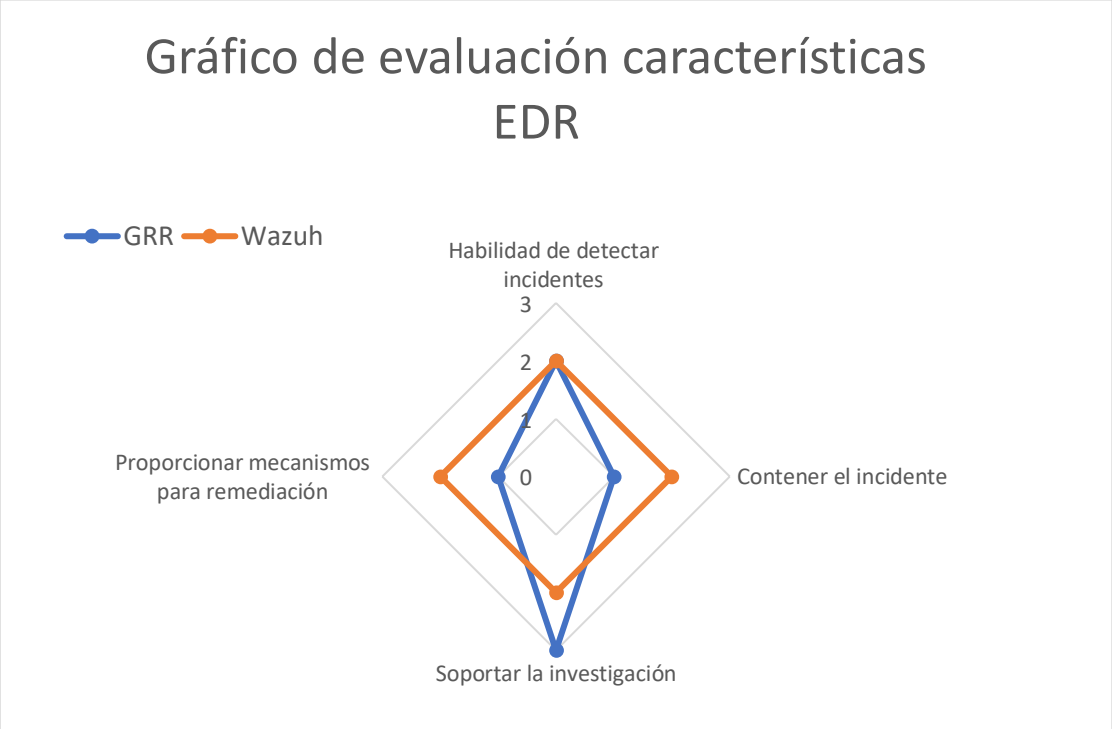


Ilustración 33. Evaluación de características EDR

Es importante tener en cuenta, que aquellas ponderaciones en el nivel relacionado como “No satisface”, hace referencia a que la herramienta nativamente no efectua la característica, no obstante sus alcances tienen valía en la ejecución de tareas automatizadas a través de otro software o de soluciones que requieren intervención humana o de tipo manual.

7. Conclusiones y oportunidades de investigación

7.1 Generales y lecciones aprendidas

El impacto y proliferación de amenazas cibernéticas en la red cuya tendencia está en alza año a año, crearon la necesidad de implementar sistemas que permitan monitoreo, visibilidad, habiliten la recolección de actividades, artefactos de seguridad, y cuenten con capacidades de mitigación y remediación de incidentes en equipos y grupos de Endpoint, creándose un nuevo mercado emergente de tecnologías conocidas como Endpoint Detection and Response las cuales responden a estas demandas.

Al existir competidores en el mercado que ofrecen herramientas de seguridad a empresas, compañías de investigación de tecnología como Gartner, determinaron que un sistema EDR debe responder a cuatro características las cuales definen este segmento de soluciones dentro del panorama de seguridad. Actualmente estos sistemas de tipo comercial son desarrollados, evaluados y contrastados respecto a estos criterios.

No obstante, cuando hablamos de tecnología siempre existe una perspectiva de desarrollo de código libre, abierto y sin fines de lucro, en el que participan y colaboran diversos actores; grandes compañías como Google y Facebook, entre otras, además de desarrolladores independientes y la comunidad de seguridad, han contribuido con la construcción de soluciones que fortalecen los procesos, ciclo de vida y fases de respuesta ante un incidente y su investigación, siendo estos sistemas catalogados dentro del conjunto de soluciones EDR. Este trabajo constituyó una revisión del estado del arte referente a estos proyectos tipo open-source que pueden destacarse en el panorama tecnológico, que responden a estos requerimientos y están dotados con estas funcionalidades.

El trabajo desarrollado abarcó en detalle dos (2) de estos sistemas, verificando su funcionamiento a través de pruebas con una muestra de malware real tipo Emotet, comprobando para éstos su capacidad y posibles funcionalidades complementarías, como la detección de actividades de tipo comportamental, específicamente de comandos Powershell, y cuyos eventos pueden pasar por alto ante soluciones de seguridad basadas en firmas como es el caso de Antivirus, entre otras tecnologías.

La experimentación proporcionó elementos para presentar una medida de la suficiencia de estos sistemas respecto a las características que debe cumplir un EDR de acuerdo con Gartner (Como son desarrollados y evaluados estos sistemas actualmente); si bien GRR y Wazuh, que fueron los sistemas escogidos como parte de las fases de investigación detallada y pruebas del presente trabajo, cubren estos apartados con diferentes grados de suficiencia ponderados y registrados en la escala creada, es importante mencionar que estos no fueron diseñados en base a estas características (Gartner), ni buscando crearse una solución EDR, no obstante poseen varias

funcionalidades relacionadas para que estos sistemas sean clasificados dentro de este tipo de soluciones.

El enfoque y metodología adoptada hacen del trabajo un proceso reproducible que puede ser usado a fin de evaluar las herramientas adicionales parte del estado del arte identificado y que, por limitaciones en términos de tiempo no fueron incluidas en detalle y alcance de este trabajo.

7.2 En relación con el cumplimiento de los objetivos

Tanto el objetivo general como los específicos planteados, fueron cubiertos con éxito durante desarrollo de la metodología planteada, al expresarse un enfoque y abordaje del tema central de manera teórico-práctica, pasando de la investigación a la implementación de sistemas y la ejecución de pruebas en un entorno controlado que involucró una amenaza cibernética real reciente, como insumo para obtener conclusiones y evaluar los grados de cercanía que pueden tener los sistemas open-source revisados en detalle, en contraste con las diferentes características a las cuales debe responder un sistema EDR mencionadas por Gartner.

7.3 De la planificación y metodología adoptada

En general la metodología y planificación planteadas fueron cumplidas de acuerdo con el plan propuesto para cada etapa expresada en la estructura de desglose diseñada para el desarrollo del trabajo. Se materializó el riesgo “Dificultades en la construcción de sistemas” que fue enunciado durante la etapa de planificación, ya que se presentaron problemas durante la implementación y puesta a punto de Wazuh para el desarrollo de la PoC; la herramienta se integró con una serie de reglas de alertamiento en seguridad leídas desde el log de Sysmon las cuales no estaban siendo interpretadas por el servidor de Wazuh correctamente, y que implicaban pérdida de visibilidad de los eventos críticos de seguridad en la consola gráfica de Kibana, esto conllevó a un retraso que se vio reflejado en limitaciones para la presentación de resultados del tercer hito de la investigación de acuerdo con la planificación inicial, lo que se percibía como un riesgo sensible frente a la conclusión del trabajo, no obstante, la eventualidad presentada fue revisada en detalle refinando las reglas de alertamiento y superando el impase, lo que permitió completar las pruebas de la herramienta y obtener las conclusiones finales registradas en este Trabajo Final de Máster.

7.4 Oportunidades de investigación y trabajo futuro

- Por la limitante de tiempo (un semestre) destinado para el desarrollo del trabajo, fue posible únicamente profundizar en dos de los sistemas que se consideraron más representativos revisando la teoría y su implementación práctica para el desarrollo de la PoC, una oportunidad futura que puede ayudar a robustecer este trabajo, es la inclusión de las demás herramientas identificadas para ser probadas y medidas bajo la metodología ejecutada en este análisis; abriendo incluso espacios comparativos para determinar cual(es) herramienta(s) puede satisfacer

mejor las características de un EDR y/o aquellas que pueden ser usadas en conjunto como una solución competitiva frente a los sistemas ofrecidos comercialmente.

- Por otra parte, estos sistemas tenían capacidades para monitorear sistemas Mac OSX y diversas variantes de Linux, un desarrollo a futuro que puede complementar el presente trabajo, sería el testeo en estos sistemas operativos frente a una amenaza cibernética común que puede ser la misma empleada en este caso, Emotet.

- Al disponer de diversas categorizaciones de malware, otra oportunidad futura que puede desprenderse de este trabajo es la realización de pruebas con muestras de ransomware, virus, gusanos, rootkits, familias de RAT[22] y spyware, entre otras amenazas de seguridad; cada una tiene características y comportamientos específicos con lo cual valdría la pena extender los ensayos a estos tipos de software malicioso.

- Una oportunidad final de trabajo se destaca en términos de desarrollo y construcción de software, en cuanto a la elaboración de reglas preestablecidas que puedan robustecer de manera rápida las capacidades de las soluciones open-source estudiadas, y que incluso pueden llegar a ser compatibles con los otros sistemas que fueron identificados. Por otra parte, dado que los sistemas estudiados (Y posiblemente los que faltan por revisar) a detalle tienen oportunidades de mejora que puedan satisfacer mejor las características de un EDR, la invitación en este caso es que codificadores y la comunidad de seguridad efectúen extensiones y desarrollo de módulos que puedan mejorar las capacidades de los proyectos actuales, como por ejemplo la habilidad de conectarse en vivo (Live) a los Endpoint monitoreados, que es una valiosa funcionalidad ofrecida por diversos EDR de tipo comercial.

[22] Remote Access Trojan

8. Glosario

- **Cryptojacking:** Uso no autorizado de las capacidades de procesamiento de estaciones de trabajo y servidores para el minado de transacciones efectuadas entre criptomonedas

- **DDoS:** Es el acrónimo de Distributed Denial of Service, es un tipo de ataque que consiste en desbordar la capacidad de respuesta de un sistema informático a través del envío de flujos y paquetes de datos con una volumetría que ocupa los puertos y capacidades contestar las solicitudes, causando su indisponibilidad.

- **Dirección IP:** Un conjunto de 4 números separados por puntos que identifica de manera lógica una interfaz y localización de un dispositivo que hace parte de una red de computadores, IP es el acrónimo de Internet Protocol, que corresponde a un protocolo de comunicaciones ubicado en el nivel de Red del modelo TCP/IP.

- **EDR:** Endpoint Detection and Response, soluciones que registran y almacenan el comportamiento a nivel del Endpoint, utilizan diversas técnicas de análisis de datos para detectar comportamientos sospechosos del sistema, suministrar información contextual, bloquear actividades maliciosas y proporcionar sugerencias de remediación para restaurar sistemas afectados.

- **EDT:** Acrónimo de Estructura de Desglose de Trabajo (Work Basic Structure WBS en inglés), es una herramienta de gestión de proyectos que reúne todo el trabajo necesario para completar un proyecto basado en hitos y entregables.

- **Endpoint:** Cualquier dispositivo con capacidades de poseer una dirección IP permitida para interactuar al interior de una organización.

- **Gartner:** Es una firma global que se dedica a la investigación y brinda asesoramiento e información relevante para la toma de decisiones estratégica de las organizaciones en finanzas, recursos humanos, servicio al cliente, mercadeo, cumplimiento regulatorio y tecnología.

- **GRR:** Google Rapid Response, solución de seguridad enfocada a la recolección e investigación de información sobre Endpoints en forma remota.

- **IBM:** Acrónimo de la empresa americana International Business Machines Corporation.

- **IoT:** Denominación que se ha proporcionado a los objetos de la cotidianidad que tienen una interfaz o conexión que les permite hacer parte de Internet, ser reconocidos en una red y tener la capacidad de enviar y recibir flujos de datos.

- **Malware:** Hace referencia al tipo de software maligno que busca afectar un sistema informático permitiendo su acceso u otros tipos de acciones no consentidas por el dueño del sistema y/o su información almacenada.

- **Phishing:** Es un concepto informático que involucra técnicas de engaño mediante la suplantación de un usuario u organización de confianza a la víctima como puede ser su entidad bancaría, para solicitar información de tipo confidencial como claves de acceso a sistemas, información de tarjetas de crédito, entre otros.

- **PoC:** Acrónimo de Proof of Concept, lo que traduce al español como "Prueba de Concepto". Es la realización de un método o idea para demostrar su viabilidad, busca comprobar a través de un experimento acotado y práctico, las potencialidades de implementación futura de una solución a través de un proyecto.

- **Powershell:** Marco de trabajo para la administración y automatización de tareas de Microsoft, consistente en una consola de comandos y un lenguaje de scripting o algorítmico asociado.

- **Fileless malware:** Amenazas maliciosas cuya ejecución no se basa en la copia y lectura de información desde un archivo alojado en un soporte de largo plazo como el disco duro de un sistema, sino que su código es interpretado directamente desde la memoria RAM.

- **Ransomware:** Subcategoría de software malicioso que cifra e impide el acceso a documentos creados por el usuario de un sistema informático solicitando el pago de una extorsión mediante criptomonedas para recibir una clave para recuperar la legibilidad de los datos.

- **Threat hunting:** Concepto traducido al castellano como “caza de amenazas”, consiste en la búsqueda de actividad anormal en servidores y estaciones de trabajo que pueden significar signos de compromiso en seguridad como intrusiones o exfiltración de datos.

- **Troyano:** Un caballo de Troya o troyano es un tipo de malware que busca percibirse ante el usuario como software legítimo o que no realiza acciones maliciosas, son usados como parte de penetraciones a sistemas con fines de espionaje, acceso, manipulación de objetos remotamente y robo de información, entre otros.

- **Open-source:** Traducido al castellano como código abierto, es un término de tecnología que se refiere al tipo de software en el cual su código es liberado para implementación sin ánimo de lucra y con posibilidades de modificaciones al mismo.

9. Bibliografía

CimSweep Project. [En línea]. [Consulta 20 de octubre de 2019]. https://github.com/PowerShellMafia/CimSweep

DA CUNHA, Iria. El trabajo de fin de grado y de máster: Redacción, defensa y publicación. Universitat Oberta de Catalunya.

EXCELSIOR, Exigen a Pemex 4.9 millones de dólares; ciberdelincuentes demandan pago. [En línea]. [Consulta 18 de noviembre de 2019]. https://www.excelsior.com.mx/nacional/exigen-a-pemex-49-millones-de-dolares-ciberdelincuentes-demandan-pago/1347395

Exigen a Pemex 4.9 millones de dólares; ciberdelincuentes demandan pago. [En línea]. [Consulta 3 de diciembre de 2019]. https://www.excelsior.com.mx/nacional/exigen-a-pemex-49-millones-de-dolares-ciberdelincuentes-demandan-pago/1347395

GARTNER, Reviews for Endpoint Detection and Response Solution. [En línea]. [Consulta 19 de septiembre de 2019]. https://www.gartner.com/reviews/market/endpoint-detection-and-response-solutions

MALWAREBYTES, Hablemos del malware Emotet. [En línea]. [Consulta 22 de noviembre de 2019]. https://es.malwarebytes.com/emotet/

TheHive Project. [En línea]. [Consulta 22 de octubre de 2019].
https://thehive-project.org/

Microsoft Sysinternals, System Monitor (Sysmon). [En línea]. [Consulta 20 de noviembre de 2019]. https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

MIG - Mozilla Investigator. [En línea]. [Consulta 18 de octubre de 2019].
https://mig.mozilla.org/

Google Rapid Response GRR Project. [En línea]. [Consulta 18 de octubre de 2019].
https://github.com/google/grr

Osquery Project. [En línea]. [Consulta 23 de octubre de 2019]. https://osquery.io/

sysmon-config | A Sysmon configuration file for everybody to fork. [En línea]. [Consulta 16 de diciembre de 2019].
https://github.com/SwiftOnSecurity/sysmon-config

Sysmon - Wazuh Sigma Rules. [En línea]. [Consulta 16 de diciembre de 2019].
https://github.com/sametsazak/sysmon

The greatest heist of the century: hackers stole $1 bln. [En línea]. [Consulta 18 de diciembre de 2019].
https://www.kaspersky.com/blog/billion-dollar-apt-carbanak/7519/

Telefonica Tells Employees to Shut Down Computers Amid Massive Ransomware Outbreak. [En línea]. [Consulta 18 de diciembre de 2019].
https://www.bleepingcomputer.com/news/security/telefonica-tells-employees-to-shut-down-computers-amid-massive-ransomware-outbreak/

TITTEL, Ed. SINGH, Gajraj. Endpoint Detection and Response for Dummies. Editorial John Wiley & Sons, Inc. USA. 2016.

PONEMON INSTITUTE, IBM SECURITY, Cost of a Data Breach Report 2019. [En línea]. [Consulta 19 de septiembre de 2019]. https://databreachcalculator.mybluemix.net/

Velocidex Project. [En línea]. [Consulta 3 de diciembre de 2019]. https://www.velocidex.com/

Wazuh Project. [En línea]. [Consulta 25 de octubre de 2019].
https://wazuh.com/