



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

EL ANÁLISIS DE MALWARE EN REDES CORPORATIVAS AISLADAS

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Iván Otero Díaz

TUTOR: Luis Álvarez Sabucedo

CURSO ACADÉMICO: 2023-2024

Universida_{de}Vigo

RESUMEN

Este trabajo propone un enfoque integral para fortalecer la ciberdefensa en las Fuerzas Armadas, centrado en la implementación de una Plataforma de Análisis Controlado de Amenazas sustentado en el análisis multimotor que dé servicio a las redes de trabajo acreditadas y aisladas.

El sistema propuesto integra la capacitación del personal, un eficiente mecanismo de reporte de alertas semiautomático, y un sistema de cuarentena y análisis para mejorar la detección temprana de amenazas. La participación de los usuarios de la red como sensores humanos distribuidos en la gestión proactiva de artefactos sospechosos constituirá una capa adicional de seguridad de las redes de trabajo acreditadas.

La evaluación de la reputación de archivos basada en las interacciones de nuestro personal se convierte en un criterio clave aprovechando la cantidad de reenvíos y las detecciones de los diferentes motores de antimalware comerciales. Además, el sistema recopila y presenta reportes de análisis de múltiples motores, proporcionando una visión colectiva de las amenazas a nivel de usuario y también específicos para los administradores de seguridad. Adicionalmente, archiva de forma segura los archivos sospechosos anteriores y es capaz de informar cuando existen cambios en la evaluación de la amenaza debidos a la actualización de las firmas de detección.

Este enfoque integral pretende constituirse en una estrategia efectiva para mejorar la defensa digital de las redes operacionales militares aprovechando la proactividad de los usuarios y los avances tecnológicos para enfrentar amenazas en constante evolución. Todo ello, sin comprometer su acreditación ni el aislamiento que tan efectivo, para defender infraestructuras digitales, ha demostrado ser.

PALABRAS CLAVE

Ciberdefensa, Análisis Multimotor, Concienciación, Redes Aisladas, Malware.

ABSTRACT

This paper proposes a comprehensive approach to strengthen cyber defense in the Armed Forces, centered on the implementation of a Controlled Analysis Threat Platform based on multi-engine analysis intended to provide service to accredited and isolated networks.

The proposed system integrates personnel training, an efficient semi-automated alert reporting mechanism, and a quarantine and analysis system to improve early threat detection. The involvement of network users as distributed human sensors in the proactive management of suspicious artifacts will conform an additional layer of security for accredited networks.

File reputation assessment based on the interactions of our staff becomes a key criterion by leveraging the number of forwards and detections from different commercial anti-malware engines. In addition, the system collects and presents analysis reports from multiple engines, providing a collective view of threats at the user level and also specific to security administrators. Additionally, it securely archives previous suspicious files and is able to report when there are changes in threat assessment due to updated detection signatures.

This comprehensive approach aims to be an effective strategy to improve the digital defense of military operational networks, taking advantage of user proactivity and technological advances to face constantly evolving threats. All this, without compromising its accreditation or the isolation that has proven to be so effective in defending digital infrastructures.

KEYWORDS

Cyber Defense, Multi-Engine Analysis, Awareness, Isolated Networks, Malware.

RESUMO

Este traballo propón un enfoque integral para reforzar a ciberdefensa nas Forzas Armadas, centrado na implantación dunha Plataforma de Análise Controlado de Ameazas baseada na análise multimotor dun servizo que atenda as redes de traballo illadas e acreditadas.

O sistema proposto integra a formación do persoal, un eficiente mecanismo de notificación de alertas semiautomáticas e un sistema de corentena e análise para mellorar a detección precoz das ameazas. A participación dos usuarios da rede como sensores humanos distribuídos na xestión proactiva de artefactos sospeitosos constituirá unha capa adicional de seguridade para as redes de traballo acreditadas.

Avaliar a reputación dos ficheiros en función das interaccións do noso persoal convértese nun criterio clave ao aproveitar o número de reenvíos e deteccións de diferentes motores anti-malware comerciais. Ademais, o sistema recolle e presenta informes de análise dos motores, proporcionando unha visión colectiva das ameazas a nivel de usuario, así como doutras específicas para os administradores de seguridade. Tamén, arquiva de forma segura os ficheiros sospeitosos anteriores e pode informar cando hai cambios na avaliación da ameaza debido ás actualizacións das sinaturas de detección.

Este enfoque integral pretende converterse nunha estratexia eficaz para mellorar a defensa dixital das redes operativas militares aproveitando a proactividade dos usuarios e os avances tecnolóxicos para afrontar ameazas en constante evolución. Todo iso, sen comprometer a súa acreditación nin o illamento que tan eficaz demostrou ser na defensa das infraestruturas dixitais.

PALABRAS CLAVE

Ciberdefensa, análise multimotor, concienciación, redes illadas, malware.

Contenido

1.	Introducción	4
1.1	Contexto	5
1.2	Objetivo	6
1.3	Estructura del trabajo y metodología.....	7
2.	Luchando contra el <i>malware</i>	10
2.1	Servicios antimalware de un COS	12
2.1.1	Análisis de malware	13
2.1.2	Análisis forense	14
2.2	Los usuarios como eslabón más débil	15
2.2.1	Concepto de red resiliente	17
2.2.2	Red de usuarios concienciados: método de alerta y detección	18
2.3	Gestión de la inteligencia corporativa	19
2.4	Servicio central de fusión de datos y generación de Intel.	20
3.	Particularidades de las redes corporativas aisladas y acreditadas.....	22
3.1	La seguridad de la información	22
3.2	Las redes acreditadas	25
3.3	Las herramientas de seguridad	26
3.3.1	Los antivirus	27
3.3.2	HIDS y NIDS como métodos de detección y alerta temprana.	30
3.4	Sistemas de Información y Gestión de Eventos de Seguridad	32
3.5	Cuadro comparativo de soluciones corporativas y sus fortalezas	33
4.	Propuesta alternativa.....	36
4.1	Casos de uso	37
4.1.1	Bloque de interacción con el usuario.	40
4.1.2	Procedimiento de actualización de motores/Sistema de exclusas.	42
4.1.3	Backend.....	44
4.1.4	Detección de APT y otras amenazas específicas contra nuestros intereses. ...	45
4.2	Tecnologías escogidas para el sistema final	47
5.	Conclusiones, nuevas líneas de trabajo y otros usos posibles.....	50
6.	Bibliografía	54

Índice de Figuras

Figura 1 - Historia del Malware y sus corrientes motivacionales	12
Figura 2 – Servicios principales de un COS. Fuente: Sernivel3	13
Figura 3 – Efectos de la gamificación en los empleados. Fuente: Zippia Research Team. .	17
Figura 4 - Ciclo de vida de la seguridad. Fuente: Rockwell Automation	25
Figura 5 – Detección híbrida de virus en nube. Fuente: Elaboración propia.	30
Figura 6 - Agentes NIDS en elementos de red. Fuente: Pro Resources Technology	31
Figura 7 - Agentes HIDS en servidores y endpoints. Fuente: Pro Resources Technology ..	32
Figura 8 - Diagrama de Casos de Uso. Fuente: Elaboración propia	38

1. INTRODUCCIÓN

La digitalización de las sociedades es un hecho indiscutible. En la práctica, todos estamos conectados y mantenemos una presencia digital en multitud de plataformas, desde sitios web hasta redes sociales, pasando por sistemas de asistencia virtual como Alexa o Google Home. Además, se está convirtiendo en norma que nuestros dispositivos cotidianos, como robots de cocina, termostatos, calderas, cerraduras inteligentes y frigoríficos, se comercialicen incorporando funciones supuestamente avanzadas derivadas de su conexión constante a servicios en nube.

Los dispositivos que conforman los entornos corporativos han experimentado la misma tendencia y las organizaciones afrontan una amenaza constante procedente del ciberespacio. La proliferación del malware ha alcanzado proporciones alarmantes, generando pérdidas financieras colosales y desafiando la integridad de los sistemas informáticos. Según un informe de Accenture, el costo promedio de un ataque de malware para una empresa es de 2.4 millones de dólares y el 64% de las empresas encuestadas experimentaron un aumento en la frecuencia de los ataques de malware durante el año anterior [1].

Dependiendo del tipo de organización lo más alarmante es, o bien el robo de datos sensibles o el impacto negativo inicial en las finanzas y posteriormente en la confianza de sus clientes y la reputación corporativa. Aplicado a las redes de trabajo de unas Fuerzas Armadas, se derivan consecuencias que erosionan su resiliencia, definida aquí como la necesidad de seguir operando sin interrupción y con unas capacidades mínimas que garanticen el cumplimiento de la tarea encomendada. Esto en última instancia implica el compromiso de su misión, que es la defensa nacional.

Con el objetivo de mitigar estos efectos cada año se invierten, tanto en organizaciones privadas como en las públicas, cantidades astronómicas en medidas de seguridad, antivirus, y programas de concienciación para protegerse contra las amenazas más peligrosas. Gracias a estas campañas de información y concienciación, la sociedad en conjunto y los trabajadores de instituciones especialmente sensibilizadas, han tomado

conciencia de los peligros que pueden afectarles en su día a día, y a los organismos para los que trabajan cuando son víctimas de una campaña en sus puestos de trabajo. Dentro de estos peligros digitales y en el contexto de este trabajo nos vamos a centrar en los más dañinos, por persistentes o por destructivos, que llevan aparejado el uso de *malware*.

1.1 Contexto

El objetivo primordial de unas fuerzas armadas es la de asegurar y defender el territorio, de manera que las fuerzas propias puedan hacer uso de él mientras se le niega el acceso y la libertad de movimiento al adversario. Para poder llevar a buen fin este cometido, los ejércitos no dejan de planear y de adaptar sus combatientes y sus equipos a los cursos de acción que con más probabilidad va a adoptar el enemigo y a las nuevas amenazas que surgen como consecuencia de los avances tecnológicos. El territorio a conformar para servir a los intereses propios no es solo físico, sino que las comunicaciones y los datos ya se han constituido como un campo de batalla específico y por ello, en el presente trabajo nos hemos querido centrar en aquellas campañas que afectan a las organizaciones a través del ciberespacio. En concreto, en las instituciones públicas que tienen redes corporativas extensas y cuyo mecanismo de defensa más efectivo es, sin lugar a duda, el aislamiento de otras redes. En ellas, una amenaza materializada puede poner en peligro la existencia de la institución y aunque las corporaciones han invertido en la concienciación de sus trabajadores y en la detección de los tipos de amenazas más dañinas para sus intereses, no han sido capaces de dotar a su personal de un mecanismo de alerta global efectivo cuando detectan una anomalía.

En una red privada con más de doscientos mil usuarios, como puede ser la de un ministerio, aunque algunos eliminan una amenaza que acaba de materializarse en sus dispositivos, muchos otros no lo harán y podrían comprometer la red entera. Esto puede evitarse si los usuarios que, tras años de cursos y campañas de concienciación, ya están convenientemente instruidos en detectar estas amenazas dispusiesen de un mecanismo cómodo de análisis y reporte automático a su disposición. Un sistema más sofisticado que el del antivirus tradicional que con total seguridad, por ser de obligado cumplimiento en redes acreditadas, tienen instalado en sus máquinas de trabajo.

En este ambiente de constante cautela digital, surge la idea fundamental que inspira este trabajo: un enfoque integral, basado en un sistema de análisis multimotor y diseñado para una protección más exhaustiva de las redes de nuestra organización contra el malware. La premisa subyacente es que la combinación de tecnologías de vanguardia, procesos sólidos automatizados y la colaboración efectiva puede no solo prevenir ataques, sino también mitigar eficazmente las consecuencias de aquellos que logran traspasar las defensas iniciales. Es por lo que la hipótesis de trabajo que se pretende demostrar en este trabajo es la siguiente:

“El personal de unas Fuerzas Armadas modernas que está capacitado para detectar anomalías y posibles amenazas en la red de trabajo también es capaz de generar alertas. La creación de un servicio que acepte estas alertas y procese los

archivos sospechosos a un análisis de malware automático, multi motor y alojado en nuestras instalaciones es la manera más efectiva de asegurar la confidencialidad de la información que se genera en una red corporativa.”

1.2 Objetivo

El objetivo del trabajo es diseñar una solución de seguridad digital que añada una capa adicional basada en el capital humano a partir del análisis de la amenazas más perniciosas y usando herramientas de seguridad preexistentes. Este sistema se denominará Plataforma de Análisis Controlado de Amenazas.

Antes de sumergirnos en los detalles de nuestro sistema y basándonos en la hipótesis planteada anteriormente, conviene fijar una serie de afirmaciones a modo de axiomas que a nuestro juicio no necesitan de mayor demostración.

- La colaboración y la diversidad de enfoques son esenciales para abordar las amenazas digitales en evolución constante.
- La implementación de tecnologías avanzadas, como el análisis con múltiples soluciones comerciales en lugar de una sola, ofrece una capa de protección adicional.
- La búsqueda de sinergias a través del intercambio de inteligencia y la colaboración con otras entidades gubernamentales pueden elevar el nivel de las defensas digitales de las redes de trabajo.

Para alcanzar el objetivo global propuesto se identifican una serie de hitos parciales cuyo estudio contribuirá a la meta final:

1. Estudio de las medidas de seguridad de nuestras redes acreditadas.
2. Estudio de las herramientas actuales para enfrentarnos al malware.
3. Fortalezas y debilidades de las familias de herramientas comerciales.

A medida que desglosemos cada aspecto del sistema propuesto, exploraremos cómo transformar las premisas en combinación con los objetivos parciales en medidas tangibles a la vez que se resuelven las derivadas de segundo orden, aunque de forma somera, que surjan a lo largo del presente trabajo.

Se aborda, por ejemplo, la capacitación del personal como pilar fundamental de nuestro Sistema y se propone desarrollar un programa que habilite a los miembros de las Fuerzas Armadas para identificar anomalías y posibles amenazas en la red de trabajo de manera que se mejore la resiliencia ante ataques ciber y se fomente una cultura de seguridad digital entre el personal militar.

Para optimizar la detección temprana de posibles amenazas, se plantea el diseño de un mecanismo eficiente de reporte de alertas. Esto implica la creación de una interfaz de usuario accesible y sencillo que permita a los usuarios reportar archivos sospechosos de manera rápida y efectiva. La implementación de esta herramienta se alinea con la premisa de que la participación proactiva de los usuarios fortalece la red, convirtiéndolos en sensores humanos distribuidos y añadiendo una capa extra de alerta.

La gestión de archivos sospechosos se presta a través de una Plataforma de cuarentena y análisis automático. Este mecanismo no solo almacena archivos sospechosos de forma cifrada, sino que también los envía a un análisis automatizado mediante múltiples motores de detección de malware que evitan los análisis innecesarios y redundantes. Este enfoque garantiza que los recursos se utilicen de manera eficiente y no se malgaste capacidad de cómputo en analizar muestras que ya han sido evaluadas anteriormente.

En paralelo, se propone el desarrollo de un sistema que evalúe la reputación de archivos sospechosos basándose en la cantidad de usuarios que lo reportan y las detecciones de los motores antimalware. Los conocimientos adquiridos por nuestro personal y sus sospechas se convierten así en un criterio clave para determinar la potencial peligrosidad de los ficheros, ofreciendo una visión más completa del riesgo asociado a archivos específicos.

Otra parte esencial del sistema propuesto consiste en la generación de reportes de análisis comprensibles para el personal lego. Se propone un módulo que recopile y presente los reportes de análisis provenientes de múltiples motores de antimalware de forma clara y estructurada. Esta información instantánea permitirá a los usuarios tomar decisiones informadas basadas en la evaluación colectiva de las amenazas sin poner en peligro la confidencialidad de sus documentos de trabajo.

El proceso se completa con la consideración de la actualización segura, desde el punto de vista de las operaciones cotidianas de la organización, de las bases de datos de firmas de antivirus gracias a un proceso automático y crucial para evitar exponer la red a amenazas externas y la exfiltración involuntaria de información clasificada. Por último, se propone establecer un sistema de notificación que informe a los usuarios que han reportado archivos sospechosos en caso de que cambie la evaluación del riesgo. Gracias a ello se potenciará su compromiso con la organización al mantenerlos informados sobre la evolución de las amenazas detectadas, premiando su constancia y acierto a la hora de alertar al resto del Sistema.

1.3 Estructura del trabajo y metodología

En el presente documento no se utiliza ningún tipo de fuente ni dato clasificado, por lo que todo el trabajo es de acceso público y se puede referenciar. Además, se centra en redes nacionales bajo la normativa ratificada por la Organización Nacional de Seguridad (ONS), aunque las de cualquier país OTAN servirían ya que compartimos unos criterios mínimos (NATO, 2015) a la hora de diseñar y generar infraestructuras de red aliadas.

La metodología elegida para abordar esta hipótesis es la de casos de uso, una herramienta de desarrollo metodológico que no solo permite desglosar el proceso de análisis y diseño en componentes manejables, sino que también facilita la comprensión de las interconexiones y dependencias dentro del sistema propuesto. Desde la identificación temprana de amenazas hasta la presentación en cuadros de mando y la respuesta coordinada, cada caso de uso se convierte en una caja negra funcional que será

esencial en la construcción completa de la Plataforma de Análisis Controlado de Amenazas.

En primer lugar, se ha abordado en el capítulo 2, Luchando contra el *malware*, la problemática a la que nos enfrentamos simplemente por tener presencia digital y cuáles son los servicios genéricos y herramientas software de los Centros de Operaciones de Seguridad con los que las corporaciones cuentan para protegerse.

En el capítulo 3, Particularidades de las redes corporativas aisladas y acreditadas, se hace un análisis más profundo de las medidas actuales de protección de aquellas redes que son vitales para las corporaciones y de los sistemas de mitigación que implementan, como el aislamiento de redes de terceros. Esta protección tan efectiva es a la vez un problema si queremos usar servicios antimalware comerciales ya que, cada vez más a menudo, ofrecen sus servicios de manera deslocalizada para todos sus clientes gracias a nubes privadas comerciales, sin un control real por parte del usuario de la privacidad de sus datos internos.

En el capítulo 4, Propuesta alternativa, se esboza el sistema propuesto a través de una serie de casos de uso que, a juicio del autor, son necesarios para modelar los protocolos, los procedimientos y el tipo de herramientas que unas Fuerzas Armadas como las españolas demandan actualmente.

Para finalizar, en el capítulo Conclusiones, nuevas líneas de trabajo y otros usos posibles se repasan las ideas fuerza desarrolladas a lo largo del trabajo y además se aprovecha para proponer líneas futuras para posteriores trabajos relacionados con la Plataforma propuesta que extiendan sus capacidades y ayuden no solo a las redes del Ministerio de Defensa de España sino al resto de Ministerios y organismos de la Administración General del Estado.

2. LUCHANDO CONTRA EL MALWARE

Desde el comienzo de la historia digital existen programadores, o entusiastas, que han querido ir un paso más allá y que por curiosidad, por intereses económicos o por atesorar notoriedad, han explorado las posibilidades avanzadas y alternativas de la tecnología. El inicio de la crónica del malware podríamos fijarla en el gusano Morris y se ramifica en una interminable saga de amenazas ciber.

El concepto de que es, y qué no, una ciberarma es controvertido, pero no es discutible que el primer malware¹ se desarrolló en 1988. Robert Tappan Morris programó un gusano², un software inocente que pronto se descontroló y, de hecho, fue el primero en propagarse de forma tan efectiva que su consecuencia fue una denegación de servicio masivo de todas las computadoras conectadas a la red, marcando el primer hito en la historia del malware. Este gusano no tenía intenciones maliciosas pero su propagación incontrolable puso de manifiesto que los programas informáticos podían ser utilizados como armas silentes.

La década de los noventa estuvo marcada por la aparición frecuente de virus y troyanos que llevaron la lucha contra el malware al siguiente nivel y fomentó la aparición de múltiples empresas de antivirus. La era de los virus en las macros de los documentos ofimáticos y los troyanos ocultos en programas legítimos causó estragos en sistemas y redes por todo el planeta. De esta época son los muy conocidos y referenciados "Melissa", "CIH" (aka "Chernobyl") y "ILOVEYOU" que causaron pavor en un momento en el que Internet crecía exponencialmente mientras que los conocimientos avanzados seguían reservados a unos pocos.

¹ Años antes se había programado un malfuncionamiento lógico, pero a nivel de firmware programándolo enteramente como una imagen maliciosa. Al hablar de malware en el presente documento siempre lo hago refiriéndome a una pieza de software que infecta a otros archivos o a un S.O. entero.

² El término gusano se acuñaría años después para distinguir a un malware que por sí mismo es capaz de replicarse y extenderse por un sistema a diferencia de los virus que necesitan infectar a un archivo legítimo que lo hospede y con ello llevar a cabo las acciones que tenga programadas.

El nuevo milenio trajo consigo una nueva oleada de malware. Los gusanos como "Blaster" y "Sasser" aprovecharon vulnerabilidades del sistema operativo Windows, y mostraron cómo se podían paralizar redes enteras. También son de esta época los malware con intereses puramente económicos y la profesionalización de la ciberdelincuencia con el despliegue primero del *spyware* y luego del *ransomware*. Este último, que sigue siendo el que mayor impacto mediático tiene hoy en día, primero cifra los datos de los dispositivos y posteriormente solicita un desembolso económico a cambio de la clave para revertir el ataque. Malware como "WannaCry" y "NotPetya" son los especímenes más conocidos gracias a que algunas de sus víctimas tenían renombre mundial.

Hasta ahora hemos repasado algunos de los malware que todos podríamos haber sufrido, a nivel doméstico, como usuarios anónimos conectados a una red pública. Sin embargo, desde el comienzo de esta cronología, otras herramientas mucho más silenciosas se estaban moviendo entre bambalinas y consiguiendo los objetivos para los que habían sido programados, las Amenazas Persistentes Avanzadas (APT, por sus siglas en inglés). Estas armas software se desarrollan con motivaciones políticas o para obtener información que sirva como base para operaciones de inteligencia y el desarrollo de líneas de acción posteriores, generalmente de tipo militar. Nombres como "Stuxnet" y "Duqu" han saltado a la luz por haber sido las causantes de hacer descarrilar años enteros de investigaciones y programas estatales de países con intereses contrarios a los de las naciones que desarrollaron los APT. Lo más significativo de este tipo de amenazas es que sus objetivos son tan concretos que su difusión es bajísima y por ello pasan por debajo del radar de las compañías de antivirus durante años. Nadie es capaz de detectarlos ni con motores heurísticos ni a través de firmas, ya que siguen actuando *in the wild*³.

En el futuro la inteligencia artificial, el Internet de las Cosas (IoT) y la computación cuántica representarán nuevos desafíos que sin duda se van a incorporar a las ciberamenazas. Afortunadamente también se verá potenciada la forma de ciberdefendernos ya que la historia del malware es un reflejo del poder del ingenio humano, tanto para la creación como para la destrucción. En la imagen se muestra una línea de tiempo que representa los tipos de malware y sus motivaciones respecto a los años en que aparecieron.

³ Se ha querido dejar la expresión en inglés, por ser de uso cotidiano en la bibliografía especializada y en artículos de revistas y periódicos. Este tipo de malware tiene actualizaciones casi constantes de manera que ningún antivirus ni XDR son capaces de detectarlos.

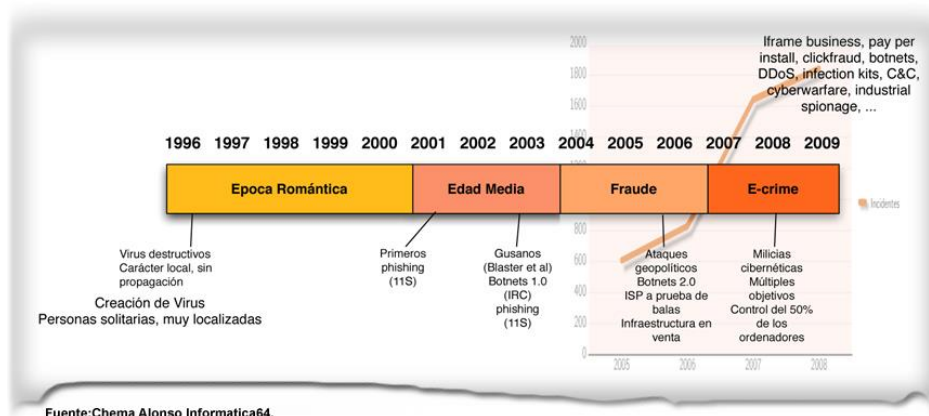


Figura 1 - Historia del Malware y sus corrientes motivacionales

2.1 Servicios antimalware de un COS

Hoy en día los servicios de seguridad de las redes corporativas suelen estar centralizados en Centros de Operaciones de Seguridad internos o externalizados. El problema cuando hablamos de redes gigantes, como la de un ministerio, es que sus servicios de seguridad, aunque pretenden ser proactivos, rápidamente se ven desbordados y se convierten en meramente reactivos. Las causas que agravan este hecho son variadas, pero en líneas generales se debe a la falta de personal especializado que pueda atender a todas las alertas generadas y a que la misma tecnología que ayuda a descartar miles de falsos positivos y descarga de trabajo al escaso personal, fracasa a la hora de enfrentarse con la amenaza más perniciosa para un Estado, los APT. Los indicios de estos malware dirigidos y personalizados para cada víctima son ignorados sistemáticamente por los SIEM y los XDR⁴ ya que los desarrolladores los programan para evitar los productos específicos que saben, por otros medios, que están instalados en la red víctima.

Dentro de los múltiples servicios que proporciona un COS, para el presente trabajo debemos destacar los dos que están más directamente implicados a la hora de combatir un APT: los servicios de análisis de malware y los de análisis forense. Estos son los encargados de diseccionar, analizar, identificar y en su caso prevenir, los ataques que se producen en una red corporativa.

Los análisis no solo se realizan sobre muestras sospechosas de un posible malware, también se incluyen aquí el rastreo en miles de líneas de logs de dispositivos de red y de eventos de seguridad detectados por todos los sistemas operativos y *firmwares* de servidores y dispositivos que conforman el sistema. Muchas de estas alarmas no serán detectadas y otras muchas serán inocuas, pero se identificarán como potencialmente maliciosas por alguno de los sensores de detección de nuestro sistema consumiendo recursos de tiempo y personal. Finalmente, un número muy reducido de ellas serán

⁴ Extended Detection and Response – Evolución de los SIEM tradicionales en los que los datos se agregan a un data lake, para lograr un logueo, búsqueda e investigación extendida más eficiente y contextualizado. A menudo también se apoya en sistemas IA.

muestras y rastros de un APT real en sus primeras etapas de intento de infección de la red y los integrantes de nuestro COS serán capaces de vislumbrarlo y luchar contra él.

Todos estos sensores suelen ser de tipo pasivo. Mientras la amenaza no se materialice o sus movimientos no empiecen a dejar huellas indebidas por los diferentes logs, probablemente nadie prestará atención, ni los sistemas de correlación de eventos lo marcaran como malicioso, hasta que sea demasiado tarde y con total seguridad el paciente cero, como poco, muera. Este hecho, además, es más evidente cuanto más grande sea la red que se pretende proteger.

En la imagen se muestra los servicios que presta un Centro de Operaciones de Seguridad interno o externalizado.

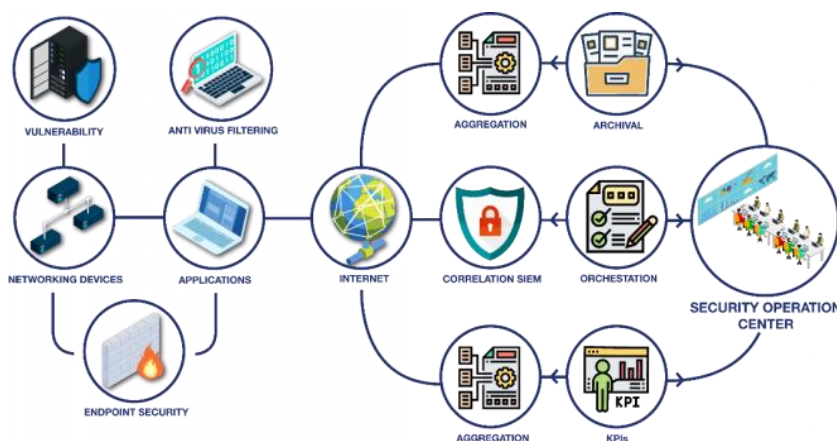


Figura 2 – Servicios principales de un COS. Fuente: Sernivel3

2.1.1 Análisis de malware

Dentro de los servicios que puede prestar un COS está, sin duda, el altamente especializado del analista de malware. Ellos son los encargados de despiezar los ejecutables revirtiendo su compilación de manera que pueden llegar a obtener el código fuente original o un pseudocódigo legible. Gracias a ellos se obtienen datos como cuál es la carga real del *payload* de un malware, cuál es su objetivo final, con que direcciones IP intenta contactar para recibir órdenes concretas, con que servidores intercambia claves de cifrado para comunicaciones seguras y encubiertas y un largo etcétera [2].

Este tipo de profesionales altamente especializados y demandados son difíciles de contratar en el mercado laboral. Su dominio de conocimiento no se imparte directamente en ninguna facultad y todo se basa en autoaprendizaje y cursos de especialización. Estos itinerarios más o menos reglados son tan caros que generalmente solo los pueden asumir las compañías como método de formación interna. Podría decirse que su trabajo es más un arte que una ciencia y retenerlos en la organización una vez formados es difícil porque la competencia entre las compañías es intensa [3]. Si, además, hablamos de una red corporativa de un organismo público donde los sueldos están limitados, este hecho se agudiza.

Al ser un tipo de profesional escaso no conviene malgastar sus horas de trabajo con muestras que claramente sean falsos positivos y se hace perentorio dotar al COS, donde trabajan, de un sistema de triaje de todas las muestras que se canalizan desde los sensores pasivos instalados en la red o externalizar este tipo de tareas a empresas que analizan malware de diversos clientes con unos pocos analistas (ver Figura 2).

Esta opción no es factible para nuestros intereses cuando el ataque está altamente dirigido contra las redes propias, por ejemplo, con un APT, ya que es a través de este análisis cuando obtendremos información de contexto sobre los verdaderos objetivos de la ciberarma y no solamente de los efectos visibles que tienen a la hora de cifrar, modificar o borrar información. Esa transformación de información sobre el adversario, elaborada y convertida en inteligencia es la que tiene un valor incalculable que no debemos compartir más que con “socios” muy fiables y nunca con una compañía de servicios a terceros [4].

2.1.2 *Análisis forense*

Un servicio de análisis forense digital es la sección encargada de recopilar y analizar las evidencias digitales en caso de incidentes de seguridad importantes para comprender el alcance y el impacto [5]. Su actividad consiste en examinar los datos almacenados en dispositivos electrónicos con el fin de identificar, preservar y recuperar información relevante para una investigación. En una red corporativa, este servicio es fundamental para proteger la integridad y confidencialidad de los documentos y datos que circulan por la red, así como para detectar y prevenir posibles ataques a través del ciberespacio.

Los profesionales que realizan este servicio también están altamente especializados en el uso de herramientas muy específicas y cuentan con conocimientos en informática, sistemas operativos, redes, criptografía y legislación. Su trabajo requiere de una metodología rigurosa y de herramientas específicas que les permitan extraer y analizar la evidencia digital sin alterarla ni comprometerla. El análisis forense digital es, por tanto, un servicio esencial para garantizar la seguridad de una red corporativa y la atribución de un ataque si hubiese que aportar pruebas válidas y trazables en caso de litigio, pero también, y especialmente en un ministerio de defensa, como base a la inteligencia corporativa que se genera sobre las amenazas digitales.

Gracias a ellos podremos saber si la pieza de malware que se encuentra es un incidente de seguridad más o una etapa de un ataque orquestado mucho mayor que afecta a la red entera y no sólo a un dispositivo. Además, en coordinación con el equipo de analistas de malware serán capaces de diferenciar si una amenaza está realmente dirigida en exclusiva contra nuestra organización y caracterizarla, para generar firmas específicas, cadenas de bytes, que identifiquen de forma inequívoca los artefactos maliciosos generados para atacar a una víctima específica. Es en esta fase donde se integra la inteligencia generada y los hallazgos técnicos en una firma para localizar sistemáticamente una amenaza concreta en nuestros sistemas.

Si bien existen en el mercado varias herramientas para gestionar estos patrones generados internamente, una de las más eficientes y que incorpora un motor de análisis con el que escanear un sistema en busca de artefactos concretos es el motor Yara⁵. Por ser de código abierto, ligero y estar ampliamente documentado es el que se utiliza de manera habitual en nuestro ministerio y en muchos otros.

2.2 Los usuarios como eslabón más débil

Los usuarios de una red son en muchas ocasiones uno de los eslabones más fácilmente atacable y efectivo para que se complete con éxito un ataque. Es en las redes con un número masivo de usuarios, altamente bastionadas y securizadas a nivel técnico, donde esta afirmación adquiere mayor relevancia por la poca superficie de ataque que ofrecen. Con el sistema propuesto a lo largo de este documento se pretende no depender únicamente de la capacitación individual de cada miembro del personal sino valerse de la "sabiduría colectiva" para descubrir amenazas añadiendo una capa extra de seguridad.

Basándonos en esta perspectiva, debemos enfocar los esfuerzos de la organización en promover la sensibilización colectiva implementando campañas de concienciación que fomenten una cultura de seguridad digital en toda la organización. Esto debe incluir la promoción de la responsabilidad compartida en la detección de amenazas a la par que se implementa un sistema de reconocimiento de méritos individual. Estas recompensas, sobre todo en prestigio, deben dirigirse a aquellos empleados que contribuyan significativamente a la detección de amenazas a la vez que se establece un mecanismo para informar a los empleados sobre las amenazas que detectaron y cómo se atajaron gracias a sus alertas.

Esta retroalimentación servirá para dirigir las futuras campañas de sensibilización y capacitación de manera que se reconozca y se aproveche la diversidad de conocimientos y experiencias de los usuarios para abordar amenazas y riesgos desde diferentes perspectivas. Otra vía de contribuir a este objetivo puede ser a través del fomento de la colaboración entre los miembros más activos, y con tasas de detección más altas, con una plataforma de colaboración que solicite una segunda confirmación sobre las sospechas de los compañeros aprovechables como parte de un sistema de formación continua en ciberseguridad y concienciación.

Esta formación continua no sólo los prepara al personal para identificar y reportar amenazas digitales, sino que también promueve la colaboración y el compromiso interpersonal [6] en la protección de las redes y sistemas corporativos al sentir que sus aportaciones se tienen en cuenta y que sus errores de percepción no van a ser desaprobados [7].

⁵ Documentación, herramienta y firmas liberadas con actualizaciones frecuentes disponible en <https://github.com/VirusTotal/yara>

El liderazgo efectivo juega también un papel fundamental en la seguridad de las redes militares. Los líderes deben personificar y promover las mejores prácticas de seguridad, estableciendo normas claras para sus equipos. Su proceder no sólo fomenta un ambiente de imitación positiva, sino que también subrayará la gravedad de la amenaza digital. Este liderazgo es un factor clave para asegurar que todos los usuarios adhieran a los protocolos establecidos y contribuyan proactivamente a la seguridad de la red por lo que es en estas figuras, líderes⁶ cercanos, para los que debemos crear también programas específicos de concienciación.

Al considerar y valorar el aprendizaje en ciberseguridad como una oportunidad para el crecimiento profesional, se motiva al personal para considerar la seguridad digital como parte integral de su deber [8], y garantiza que cada usuario actúe como un defensor indispensable de la infraestructura digital⁷, manteniendo una vigilancia constante y preparada para prevenir, o en su caso reaccionar, ante una amenaza. Se trata pues, de una dimensión cultural a potenciar y cultivar a través del aprendizaje y la concienciación en ciberseguridad en busca de un empoderamiento colectivo que enfrente a los desafíos.

La gamificación y la participación en simulacros que imitan escenarios de amenaza real son tácticas esenciales para mejorar la eficacia en la protección de las redes. Además, estos métodos han demostrado ser excelentes en otros campos militares que se practican y se aprenden de la misma manera [9].

Estos métodos aumentan la retención del conocimiento basado en la repetición de acciones y la capacidad de reacción bajo presión, al tiempo que convierten la capacitación en una experiencia más atractiva y dinámica. Los reconocimientos y las recompensas por el desempeño sobresaliente servirán de incentivos eficaces, generando un mayor compromiso con las prácticas de seguridad y una mejora continua en las habilidades de ciberdefensa [10]. Además, gracias al entrenamiento *gamificado* se estimula la colaboración y el intercambio de conocimientos entre el personal potenciando el aprendizaje colectivo. Este intercambio de información y experiencias asegurará que las lecciones aprendidas se diseminen con más facilidad a través de la organización, fomentando una base media de conocimientos sólidos y una respuesta coordinada frente a amenazas.

La integración de estos métodos en los programas de formación debería garantizar una respuesta capaz de enfrentar las amenazas actuales y asegurará una mejor preparación para adaptarse a las complejidades de las amenazas futuras.

⁶ Con líderes cercanos nos referimos a mandos intermedios, accesibles por parte de los trabajadores.

⁷ En el MDEF esta infraestructura tiene nombre propio. La denominamos I3D (Infraestructura Integral de Información del Ministerio de Defensa).

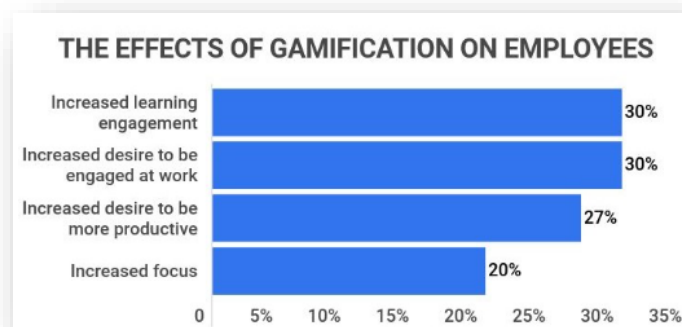


Figura 3 – Efectos de la gamificación en los empleados. Fuente: Zippia Research Team.

2.2.1 Concepto de red resiliente

En un entorno militar, la resiliencia de la red adquiere una dimensión aún más crítica que en otros entornos exclusivamente empresariales, donde las implicaciones van más allá de la eficiencia operativa y alcanzan directamente la seguridad nacional y la eficacia de las operaciones [11].

La principal aspiración de una red resiliente en el ámbito militar es asegurar que sigue siendo útil para planear y conducir las operaciones y tareas que aseguren la seguridad nacional y la integridad territorial. Estas operaciones dependen en gran medida de la transmisión segura y confiable de información. La resiliencia debe garantizar que esta información se mantenga segura y accesible, incluso con un ciberataque en curso. Las funciones de mando y control deben permanecer operativas y sin interrupciones. La red debe asegurar que las líneas de comunicación se mantienen intactas, permitiendo que las decisiones críticas y las órdenes sean comunicadas eficientemente a todos los destinatarios.

Poseer una red resiliente proporciona una ventaja táctica significativa ya que la capacidad para recuperarse rápidamente ante ataques y fallos, o poder soslayarlos sin impacto significativo por parte de los usuarios legítimos, permite a las fuerzas militares mantener su eficacia operacional frente a los adversarios. Los incidentes⁸ van a ocurrir, a pesar de las medidas de protección y mitigación implementadas, y debemos asegurar la manera en que el daño se contenga al mínimo limitando el impacto en nuestra operatividad [12].

Por último, saber que se opera dentro de un sistema de comunicación seguro y confiable fortalece la moral de nuestro personal y les permite centrarse en sus misiones sin la preocupación adicional sobre la integridad y la confidencialidad de sus comunicaciones y objetivos. En un contexto militar, la resiliencia de la red es sinónimo

⁸ No solo nos referimos a un ataque de origen en el adversario ya que debemos minimizar el impacto de los desastres naturales que causen daño físico a la infraestructura.

de supervivencia, ventaja táctica y eficacia operativa [13]. Es un elemento indispensable que subyace a todas las facetas de la planificación y ejecución militar, asegurando que, en el dominio de la información, las fuerzas armadas permanezcan siempre un paso por delante de sus adversarios.

2.2.2 Red de usuarios concienciados: método de alerta y detección

Las inversiones en concienciación de los trabajadores, tanto en dinero como en horas, se han convertido en una piedra angular para las entidades preocupadas de los peligros y amenazas digitales en constante evolución y dirigidas contra sus intereses. Decenas de programas de formación diseñados para personal con distintos niveles de conocimiento se imparten anualmente, desde orientaciones para escoger y recordar contraseñas seguras hasta la identificación visual de correos electrónicos con *phishing*. Sin embargo, a pesar de estos propósitos, el retorno de la inversión (ROI) muchas veces no es proporcional al gasto⁹. La raíz del problema yace en la carencia de un sistema ágil para transmitir a los órganos adecuados, los COS, las sospechas que los usuarios puedan tener. La concienciación es esencial, pero se vuelve incompleta si no se complementa con un análisis inicial profundo y rápido de las posibles amenazas. ¿Cómo esperar que nuestros soldados sean la primera línea de defensa contra las amenazas ciber cuando carecen de un sistema centralizado para validar o desmentir esas preocupaciones de manera inmediata?

Es en este contexto donde la visión de una red de sensores humanos distribuida emerge como una estrategia innovadora y potencialmente muy efectiva. En este trabajo se aborda la creación de una red con capacidad de razonamiento distribuido - el de nuestros empleados concienciados - dónde cada uno de ellos es un nodo en esta red, capaz de detectar amenazas potenciales y alertar al resto del sistema. Esta red de sensores humanos se convertiría en un complemento vital a las capas de seguridad existentes, especialmente en una red aislada y acreditada, altamente segmentada y bastionada.

Paradójicamente, la falta de este sistema y las altas tasas de éxito de los programas de concienciación de nuestras tropas están teniendo un efecto contrario al esperado. Documentos que nunca debieron llegar a internet lo están haciendo gracias a los empleados que esperan una confirmación de benignidad antes de abrir archivos sospechosos tal y como se explica en un informe de Blue Coat de 2015 [14]. Desde una dirección IP propiedad del ministerio de defensa español se subió al servicio online de Virustotal un documento con información sensible. Horas más tarde este mismo archivo

⁹ Al tratarse de organismos públicos sería más exacto referirse a los retornos sociales de la inversión, o SROI (siglas en inglés de “Social Return of Investment”), de manera que se pudiese evaluar la rentabilidad social y económica de las campañas de concienciación en términos de seguridad de la información generada por organismos públicos.

fue enviado de vuelta, convenientemente *weaponizado*¹⁰ con Cloud Atlas¹¹, a varias direcciones mail del Ministerio de procedencia en un intento de comenzar una infección con este APT.

2.3 Gestión de la inteligencia corporativa

En los últimos años, la importancia del intercambio de inteligencia sobre amenazas digitales entre corporaciones se ha vuelto cada vez más crucial. Sin embargo, esta práctica genera discusiones, sobre todo cuando se pertenece a alianzas militares cambiantes, con respecto al equilibrio entre los beneficios y riesgos de compartir dicha información con asociados cuyos intereses no están totalmente alineados con los propios. No es objeto de este trabajo el análisis de las mejores prácticas, ni las mejores formas, relacionadas con el intercambio de inteligencia corporativa sobre amenazas. Centrémonos pues, en las complejidades del intercambio de inteligencia sobre amenazas digitales mientras mantenemos la seguridad e integridad de nuestros documentos y no compartimos la inteligencia interna que generamos sobre nuestros adversarios.

El intercambio de inteligencia sobre amenazas es una forma eficaz para mantenerse a la vanguardia cambiante del panorama de amenazas ciber. Compartir inteligencia, es innegable, proporciona varios beneficios como una mejor conciencia situacional, una toma de decisiones más precisa y un menor riesgo de pérdida de datos [15] [16]. Las organizaciones pueden utilizarlo para evitar la pérdida de datos, proteger la información de identificación personal y reducir el riesgo de ataques ciber [17]. Se pueden utilizar varios enfoques diferentes para compartir inteligencia sobre amenazas [18], como una plataforma colaborativa, una plataforma para compartir inteligencia sobre amenazas¹² o redes para compartir inteligencia. Pero, si bien, el intercambio puede ayudar a las organizaciones a reducir los riesgos relacionados exclusivamente con el cibercrimen, también puede conllevar algunos riesgos si no se gestiona adecuadamente [19].

En el caso de una red ministerial, como es el que nos ocupa, este tipo de riesgos preocupa menos¹³ que mantener la operatividad de la red y para ayudar a las organizaciones a gestionar el riesgo, los equipos de seguridad deben adoptar un enfoque

¹⁰ Transformado en una ciberarma con la inclusión de una primera etapa infectora de recopilación de información sobre el objetivo.

¹¹ APT, también conocido como *Inception*, sucesor de “Red October”, cuya primera etapa en 2015 estaba basada en la herramienta PowerShower.

¹² España, y en concreto el MDEF, son activos usuarios de una plataforma basada en MISP en la que se comparte información sobre amenazas con aliados OTAN. A nivel nacional la plataforma REYES basada en la misma solución es la que está aprobada y ampliamente utilizada para la misma labor.

¹³ Si bien son preocupantes, las amenazas materializadas que son puras de cibercrimen, como el robo o la estafa económica al ministerio o a sus trabajadores, lo realmente importante son los ataques cuyo objetivo es paralizar las acciones del ministerio y el normal desarrollo de sus actividades. Por ello son especialmente importantes los ataques tipo APT.

de confianza cero a la hora de compartir hallazgos y conclusiones sobre incidentes en curso e intentar comprender las amenazas potenciales y sus motivaciones. De hecho, desde nuestro punto de vista, toda la información de detección de amenazas en una red de trabajo militar debería ser, por defecto, calificada como TLP: RED¹⁴. Cuando estamos bajo el ataque activo de una amenaza desconocemos si nuestro adversario tiene conocimiento de que la amenaza o alguna de sus fases previas está teniendo éxito en superar nuestras defensas. Compartir esta información puede hacer cambiar las TTP (Tácticas, Técnicas y Procedimientos) de nuestro adversario de manera que sus operaciones vuelvan a pasar inadvertidas para nuestros sensores [20].

Si bien desde un punto de vista empresarial hay ventajas a la hora de compartir información sobre amenazas, dentro de un organismo público cuyo objetivo es la defensa nacional las desventajas superan con creces el resto de los argumentos. Mientras nuestros equipos forenses y de analistas contienen la amenaza y estudian los objetivos y motivaciones del adversario conviene mantener esta persecución en secreto de manera que podamos controlar a que información, veraz o no, le dejamos acceder dentro de nuestra red.

2.4 Servicio central de fusión de datos y generación de Intel.

En una red corporativa privada de gran envergadura, asegurar la consistencia de los datos es un desafío monumental, especialmente cuando estos deben ser utilizados por múltiples Centros de Operaciones de Seguridad (COS)¹⁵ y provienen de diversas fuentes legadas. La complejidad aumenta exponencialmente a medida que la red se expande, incorporando nuevos sistemas y tecnologías sin dar de baja definitiva todo el parque anterior, generando un torrente constante de datos que debe ser procesado y entendido de manera uniforme.

En este contexto, el *Information Knowledge Management* (IKM) se convierte en un componente crítico para mantener la integridad y la coherencia de los datos recopilados y catalogados. La gestión del conocimiento trata de organizar, analizar y distribuir información de manera eficiente para tomar decisiones fundamentadas en los datos conocidos. Sin embargo, en redes corporativas extensas, el mayor desafío es, precisamente, la forma en que se estructuran los datos en diferentes partes de la red. Cada departamento, o división, utiliza formatos y denominaciones distintas y la falta de estandarización dificulta la creación de una visión unificada. Aquí es donde entra en juego la necesidad de un repositorio común, una especie de biblioteca de datos centralizada.

¹⁴ Desde agosto del 2022 la versión 2 es la aprobada por el FIRST (*Forum of Incident Response and Security Teams*) y sirve para el intercambio de información sensible pero no clasificada dentro de un entorno operativo.

¹⁵ Actualmente en el MDEF existen 4. Uno por cada ámbito y no parece que su número vaya a disminuir.

Este repositorio común no solo almacena datos, sino que debe ser concebido como un "Data Lake" corporativo. Una infraestructura de almacenamiento que permita retener todos los tipos de datos, en bruto y enriquecidos, en su formato nativo hasta que se necesiten. Esto implica que debe ser capaz de albergar datos estructurados y no estructurados, ofreciendo una plataforma flexible y escalable para la gestión de un alto volumen de datos heterogéneos, tanto históricos como en constante generación.

La implementación de un repositorio común aborda la cuestión de la coherencia y mejora la eficiencia operativa. Permite una colaboración más efectiva entre los diferentes COS al proporcionar una fuente única y autorizada de datos ciertos. Además, facilita la automatización de procesos, ya que los datos están estructurados de manera uniforme y son más accesibles para herramientas de análisis y respuesta automatizada.

En términos de seguridad, el concepto de Data Lake también puede integrarse con funciones y herramientas avanzadas. Los más modernos incorporan controles de acceso y políticas de seguridad robustas para garantizar la protección contra accesos no autorizados y manipulaciones maliciosas, crucial en un entorno donde la integridad de los datos es esencial para la toma de decisiones operativas y de seguridad.

Al adoptar un enfoque integral para la gestión del conocimiento, la organización puede aprovechar al máximo la riqueza de la información que atesora y generar inteligencia. Cuando esta inteligencia se elabore a partir de información proveniente de los sensores de seguridad y de otras fuentes de información clásica se denomina ciber inteligencia de la amenaza [4].

Algunas entidades de tipo empresarial ya han empezado a transitar por este camino, pero en otras de tipo público y con décadas de datos históricos en custodia es difícil acometer este tipo de iniciativas. Se deberá empezar, desde nuestro punto de vista, por diseñar un Data Lake que al menos aglutine y agregue la información de los sensores de detección que ya tenemos instalados en el entorno corporativo. Actualmente se cuenta con soluciones tipo XDR y SIEM que, si bien son un avance, no son capaces de cubrir todo el espectro que necesitamos para asegurar la confidencialidad de nuestras comunicaciones y de la información que generamos.

3. PARTICULARIDADES DE LAS REDES CORPORATIVAS AISLADAS Y ACREDITADAS

Hoy en día, la protección de la información es una prioridad crítica. En un ambiente empresarial la exposición de datos confidenciales puede tener consecuencias devastadoras, incluyendo la pérdida de propiedad intelectual, la fuga de datos sensibles y, en última instancia, un daño a la reputación empresarial y la pérdida de confianza. En el caso que nos ocupa para este trabajo, una red ministerial y la confidencialidad de la información que en ella se contiene, podría decirse que es aún más crítica ya que, potencialmente, toda una sociedad puede verse afectada y no solo un grupo de inversores.

Para garantizar la seguridad de la información se suelen utilizar redes aisladas (*air-gapped*¹⁶) como una estrategia de seguridad esencial. Estas redes presentan particularidades únicas, y su implementación es fundamental para salvaguardar la información crítica de una gran entidad ya que están física y lógicamente desconectadas de otras redes, especialmente de Internet. En lugar de utilizar conexiones de red convencionales, se recurre a medios aislados como dispositivos con sistemas operativos securizados y bastionados, redes locales privadas y servidores específicos y únicos para generar estas redes. La información se mueve, desde y hacia este sistema, de manera limitada y altamente controlada, generalmente a través de medios de almacenamiento físico extraíbles, como discos duros o unidades USB.

3.1 La seguridad de la información

En un mundo donde la información es un activo valioso, las redes aisladas son el componente base que sustenta la estrategia de seguridad de la información de las grandes compañías. La principal característica es su enfoque en la seguridad de los documentos

¹⁶ Este término en inglés hace referencia a que son redes que no tienen una conexión directa e ininterrumpida con otras redes por tanto existe un *gap* que hay que salvar.

que contendrá como eje central de su creación¹⁷ tras la aprobación del documento iniciático que se denomina Concepto Operacional (CO) [21]. Como decíamos, estas redes no tienen conexión directa a internet por lo que el riesgo de ataques externos se reduce significativamente y elimina una gran parte de la superficie de ataque lo que facilita mantener la integridad de los datos¹⁸ pero sobre todo coadyuva a mantener la confidencialidad de estos.

Aunque menos comunes, los ataques internos también son una preocupación para las entidades y sobre todo para aquellas con miles de empleados por una simple cuestión estadística. Si bien las redes aisladas dificultan los ataques desde el exterior, si no están bien securizadas y bastionadas, los empleados malintencionados¹⁹, los *insiders*, podrían realizar actividades no autorizadas o intentar exfiltrar información.

Una práctica habitual en algunas redes, pero obligatoria para las acreditadas es la segregación, al menos a nivel lógico, atendiendo a las diversas funciones que se desarrollen en los departamentos o a los roles de los usuarios que las utilizan. Esta segregación pretende evitar la fuga de datos.

Otro mecanismo de seguridad obligatorio es el control sobre quién puede acceder y utilizar los datos dentro de una red aislada²⁰. Esto permite una autenticación y autorización granular que disminuye el riesgo de accesos no autorizados.

Como contrapartida a tanta seguridad podemos señalar la necesidad de contar con personal especializado en seguridad y en administración de sistemas informáticos. La formación constante, la revisión y la actualización de políticas de seguridad son cruciales para mantener la eficacia de los mecanismos y las salvaguardas implantadas en una red aislada. Asimismo, la necesidad de usar medios físicos y procedimientos robustos para poder transferir datos desde una red externa (como pueden ser las actualizaciones de seguridad de los sistemas operativos) se convierten en una tarea ardua y pesada.

El siguiente paso tras el visto bueno del CO implica la realización de un exhaustivo Análisis de Riesgos (AR). En el contexto de la acreditación de un sistema de información,

¹⁷ De hecho, a la hora de generar una red para manejar información con clasificación de confidencial o mayor el primer documento que debe ser aprobado es el Concepto Operacional y en él ya se esboza el tipo de información y de seguridad que se va a implementar.

¹⁸ Es habitual en textos que tratan estos temas centrarse en la integridad de los sistemas que si bien es muy importante aún lo es más la protección de los documentos y la información que contienen.

¹⁹ Los *insiders* en redes gigantes son inevitables. Las técnicas para descubrirlos no entran dentro de los objetivos de este trabajo.

²⁰ Dependiendo del nivel de clasificación, y del riesgo asumible por el dueño de cada red, este control se puede ejercer a nivel de fichero o de directorio.

este análisis se erige como la columna vertebral que garantiza la seguridad mínima²¹ de los documentos generados y almacenados en él. Este proceso meticuloso y sistemático busca evaluar los activos de información, las vulnerabilidades, las amenazas y las posibles consecuencias de incidentes de seguridad en un sistema específico. Su propósito fundamental es proporcionar a la organización una herramienta para tomar decisiones estratégicas en la generación, mantenimiento y protección de su infraestructura tecnológica.

En la primera iteración de este análisis se recopila un inventario detallado de los activos del sistema y sus interrelaciones. No se trata sólo de una enumeración de servidores, bases de datos y dispositivos de usuario, sino que implica una valoración del valor crítico de cada activo en relación con los objetivos y funcionalidades del sistema a generar. Desde la documentación clasificada hasta los datos de usuarios, cada componente se pondera cuidadosamente para asignar los recursos necesarios para su protección dentro de unos riesgos asumibles.

Dentro de esta valoración se analizan las posibles vulnerabilidades, desde fallas en el software hasta configuraciones incorrectas de algún componente del sistema. Este análisis proactivo busca detectar debilidades antes de que puedan ser explotadas, proporcionando la ocasión de implementar medidas correctivas o mitigadoras. De la misma manera, se exploran las amenazas externas, desde ataques ciber hasta desastres naturales, permitiendo una comprensión a todos los niveles de los riesgos potenciales que podrían afectar a la continuidad de las operaciones [12].

La siguiente fase implica evaluar la probabilidad de que una amenaza explote una vulnerabilidad específica y las posibles consecuencias. Este proceso lleva a la categorización en niveles de riesgo, generando una matriz que identifica aquellos contra los que debemos protegernos en primer lugar por su nivel de criticidad en caso de materializarse. Dado que los recursos son finitos y la seguridad total es una quimera, se utiliza esta matriz para priorizar la implementación de salvaguardias y desarrollar planes de mitigación, enfocados en las áreas críticas.

Estos pasos no tienen un final ya que el análisis de riesgos se integra dentro del ciclo de vida de la seguridad representado en la Figura 4; se trata de un proceso continuo que se enfrenta a amenazas en constante evolución, actualizaciones de firmware y software de los sistemas, y vulnerabilidades que surgen con el tiempo. Por lo tanto, la revisión y actualización periódica del AR es una obligación para mantener la acreditación de un sistema a lo largo del tiempo.

²¹ La seguridad en cuanto a confidencialidad por lo restrictivo de los controles de acceso que se implementarán. Además, y dependiendo del tipo de información y la clasificación de los datos también se deberá asegurar, hasta cierto punto, la integridad y la disponibilidad.



Figura 4 - Ciclo de vida de la seguridad. Fuente: Rockwell Automation

Hasta este punto, hemos abordado la parte del cumplimiento normativo necesaria para generar un sistema de información acreditado. A continuación, exploraremos las herramientas adicionales necesarias para operar el sistema, desde sensores de anomalías hasta complejos sistemas de agregación de alarmas, con el objetivo de proporcionar una monitorización continua de los activos.

3.2 Las redes acreditadas

Las redes acreditadas son infraestructuras diseñadas de manera específica para la salvaguardia de datos de alto valor, operando en entornos que imponen exigencias extremas en términos de seguridad. La conectividad con otras redes se encuentra severamente restringida, y el acceso a la información está limitado exclusivamente a usuarios autorizados con necesidad de conocimiento. Cada aspecto de una red acreditada está fuertemente controlado y supervisado, creando un ecosistema altamente seguro que destaca por sus características distintivas y sus estrictos protocolos.

La seguridad de la información contenida constituye el fundamento de las redes acreditadas. Están diseñadas desde sus cimientos con el propósito de minimizar la superficie de ataque, lo que las hace altamente resistentes a intrusiones, y el riguroso control de acceso requiere que los usuarios se sometan a un proceso exhaustivo de autorización previo, respaldado por documentación que demuestre su idoneidad²². La segmentación avanzada se implementa para asegurar que, incluso en caso de una eventual brecha de seguridad, los atacantes tengan un acceso limitado, dividiendo la información por roles y directorios. La monitorización constante es otra de las características distintiva

²² En España, por ejemplo, las Habilitaciones Personales de Seguridad las emite la ONS.

de las redes acreditadas, con el objetivo de detectar cualquier actividad sospechosa o anómala para abordarla de inmediato.

Estos sistemas están diseñados para una respuesta rápida ante amenazas y ataques en curso, con protocolos rigurosos que permiten a los administradores tomar medidas inmediatas y automáticas para minimizar daños y contener infecciones. El cifrado robusto es obligatorio para los datos almacenados o en tránsito, dificultando considerablemente el acceso a información clasificada en caso de un incidente. Además, el mantenimiento y las actualizaciones se someten a procesos rigurosos, exigiendo la implementación ágil de parches de seguridad en softwares y firmwares²³.

Estas medidas técnicas y documentales son evaluadas mediante un proceso de acreditación llevado a cabo por organismos externos, especialmente estricto cuando estas redes gestionan información con clasificación de seguridad. En el contexto español, la Oficina Nacional de Seguridad (ONS), vinculada al Centro Nacional de Inteligencia, es la entidad acreditadora exclusiva para redes que manejan información clasificada como Reservada (equivalente a NATO Secret).

La acreditación confiere el derecho a la custodia, manejo y edición de documentos con clasificación de seguridad, siempre y cuando se mantengan las medidas de seguridad, los dispositivos estén actualizados y se cumplan todos los protocolos aprobados.

3.3 Las herramientas de seguridad

Las herramientas de seguridad desempeñan un papel crucial para mitigar riesgos y proteger los sistemas contra diversas amenazas. Los antivirus tradicionales son una primera línea de defensa preventiva obligatoria y mediante el uso de firmas y heurísticas, buscan patrones de código malicioso en archivos y actividades del sistema. A medida que las amenazas han evolucionado los antivirus han transitado hacia tecnologías basadas en nube para mantener ciclos de actualización rápidos y proporcionar protección en tiempo real sin afectar al rendimiento de los dispositivos de los usuarios.

Además de los antivirus de carácter preventivo, los programas antimalware abordan un espectro más amplio de amenazas en busca de aquellas que ya se han materializado. Estas herramientas suelen emplear tecnologías más complejas, como el análisis heurístico, el aprendizaje automático y la inteligencia artificial para identificar comportamientos sospechosos y con ello amenazas aún desconocidas. En un entorno corporativo, la combinación de antivirus y antimalware forma una defensa que se considera suficiente contra ataques digitales.

²³ Cuando las redes son muy grandes suelen contar con un entorno de preproducción en donde se puede testear que los parches y las actualizaciones no van a degradar el comportamiento normal de la red. Además, por lo general se usan versiones de sistema operativo de tipo *Long Term Support*, que aseguran el mantenimiento durante más años y con unos parches menos frecuentes que las versiones domésticas.

Para una seguridad más proactiva o en aquellas redes con información clasificada²⁴ se exige la implementación de sistemas de detección de intrusiones en el *Host*²⁵. Estos sistemas monitorizan la actividad en los dispositivos de usuario utilizando la capacidad de cómputo local, detectando comportamientos inusuales o intentos de intrusión y avisando a un recolector de eventos instalado en la red de cualquier anomalía. Además de alertar sobre actividades sospechosas, en algunos casos, también son capaces de tomar medidas correctivas automáticamente. Estos sistemas son esenciales para la identificación temprana de intentos de explotación de vulnerabilidades o amenazas internas.

En un enfoque más avanzado y para redes especialmente críticas se utilizan herramientas que despliegan señuelos o "*decoys*" monitorizados. Estos señuelos simulan activos de la red, como servidores, estaciones de trabajo o archivos con información sensible, para atraer a posibles atacantes. Al vigilar la interacción con estos señuelos se pueden identificar patrones de ataque, fortalecer las defensas y estudiar las necesidades de información del adversario. Estas herramientas no solo proporcionan una capa adicional de seguridad, sino que también permiten entender mejor las TTP adversarias ayudando a generar inteligencia de la amenaza.

Las herramientas de seguridad, por tanto, son diversas y complementarias. Desde los antivirus y antimalware que ofrecen protección esencial hasta los HIDS que brindan monitorización continua y el despliegue de señuelos que añaden una dimensión activa a la defensa. La combinación de estas tecnologías y otras como los NIDS, la segmentación de red y los productos de protección perimetral son esenciales para abordar la creciente sofisticación de las amenazas cibernéticas [22].

3.3.1 Los antivirus

En el mundo digital actual, la seguridad ya se ha convertido en un tema esencial. La proliferación de malware, virus y otras amenazas llevó, a principios de siglo, a un auge en la industria de antivirus. Las empresas de antivirus juegan un papel esencial en la protección de sistemas y datos contra amenazas digitales, y en este apartado, veremos a grandes rasgos cómo funcionan, pero sobre todo la competencia feroz que existe entre ellas.

En la era digital actual, la seguridad se ha convertido en un componente crítico que subyace en las operaciones cotidianas de forma casi transparente para nuestro personal. El vertiginoso aumento del número de amenazas a principios de siglo propulsó la industria del antivirus y en esta dinámica las empresas especializadas en antivirus emergieron como aliados fundamentales a la hora de proteger los sistemas de información.

²⁴ Hoy en día muchas empresas declaran poseer información que ellos consideran secreto empresarial. No debe confundirse con el término "información clasificada" que se usa en el presente trabajo ya que nos referimos a materias recogidas en la Ley de Secretos Oficiales (Ley 9/1968 de 5 de abril).

²⁵ HIDS – *Host Intrusion Detection System* por sus siglas en inglés.

El funcionamiento de estas herramientas no se limita a la mera detección y eliminación de amenazas, sino que también sirve para neutralizar de manera proactiva las amenazas conocidas, mediante firmas y heurísticas. La competencia entre estas empresas ha dado lugar a una carrera de innovación y adaptación constante que desemboca en la mejora continua y la distinción diferencial de sus productos y servicios.

Cada empresa busca destacarse no solo en la eficacia de su protección sino también en la eficiencia de sus soluciones y su bajo impacto en el sistema protegido. Para poder satisfacer todas estas necesidades y como la práctica totalidad de sus clientes no trabaja con documentos clasificados sus servicios dependen, cada vez más, del procesamiento en nube. Evidentemente, la inteligencia generada, convenientemente anonimizada, alimenta la base de datos que nutre a toda la red de usuarios sin que la víctima original pueda evitar su difusión.

3.3.1.1 *Funcionamiento de los Antivirus*

Los antivirus son programas informáticos diseñados para identificar, prevenir y eliminar software malicioso²⁶, de los dispositivos y sistemas. Utilizan varias técnicas para detectar amenazas, pero la principal es la comparación de los archivos a examen contra una base de datos de firmas en la que cada fabricante almacena firmas únicas del malware que ya conoce para buscar coincidencias. Esta base de datos necesita actualizaciones frecuentes²⁷ ya que un simple compilado, por parte del adversario malicioso, con *flags* de optimización²⁸ diferentes provoca cambios suficientes para que las firmas sean inservibles.

Tras unos primeros años de simples comparaciones todos empezaron a desarrollar lo que se conoce como motores heurísticos. Estos elementos buscan conductas sospechosas en lugar de firmas específicas lo que les permite detectar amenazas nuevas o desconocidas basadas en comportamiento, pero este tipo de análisis da lugar a muchas detecciones falsas por lo que en realidad acabó convertido en un sistema de *scoring*²⁹. En algunos fabricantes ahora se ha convertido en una supervisión continua del comportamiento de aplicaciones concretas para detectar cambios inusuales.

²⁶ *Malicious software* en inglés que acabó apocopándose como *malware* que es el término más comúnmente utilizado.

²⁷ Generalmente son diarias, aunque algunos fabricantes las hacen más frecuentes durante campañas específicas.

²⁸ No todos los malware están programados en lenguaje compilado, pero en otros lenguajes un simple cambio de codificación consigue los mismos efectos si el antivirus solo se basa en firmas.

²⁹ Cada acción en el sistema tiene asignada una puntuación. Cuando una aplicación suma suficientes puntos por las acciones que lleva a cabo en un periodo suficientemente corto de tiempo se marca como sospechosa y se analiza de manera más intensa, local o remotamente.

3.3.1.2 *La Competencia entre Empresas de Antivirus*

La competencia en la industria de antivirus es intensa. Las empresas luchan por demostrar que sus productos son más efectivos en la detección y eliminación de *malware* que los de sus competidores a la vez que son más livianos y menos intrusivos con los dispositivos. Como resultado, los fabricantes se encuentran inmersos en una carrera constante para mejorar y perfeccionar las tecnologías de seguridad espoleados por las comparativas de efectividad y rendimiento realizadas por entidades independientes de manera regular. Estas pruebas evalúan la capacidad de los antivirus para detectar malware conocido y desconocido, así como el impacto en los sistemas a la hora de ser examinados³⁰.

Las empresas de antivirus, hoy en día, están en constante innovación desarrollando motores heurísticos más avanzados, mejorando algoritmos y buscando nuevas formas de proteger a los usuarios³¹. Últimamente el incorporar inteligencia artificial a sus productos ya se ha convertido en un componente habitual de la detección (y sobre todo de la publicidad) en la que los antivirus utilizan aprendizaje automático para identificar patrones de comportamiento malicioso e identificar campañas completas. Lo malo, para nuestros intereses como usuarios de redes aisladas, es que esta nueva tecnología se ejecuta en una nube que no siempre es totalmente privada.

Sin embargo, no todo es competencia, la venta de firmas y motores heurísticos es una práctica común en la industria y algunas empresas especializadas en la detección de malware venden sus bases de datos de firmas³² a otros fabricantes unos días/horas más tarde de haberlas estado explotando ellos mismos. Esto permite a las empresas de antivirus fortalecer sus capacidades de detección al adquirir datos y tecnología probados además de inundar el mercado con marcas blancas de su mismo producto y ahogar a competidores pequeños.

3.3.1.3 *Modelo tradicional y modelo a futuro*

Actualmente cuando instalamos un software antivirus no debemos instalar otro en el mismo sistema. Sus motores de detección ya casi no entran en conflicto debido a los

³⁰ Alrededor del año 2010 los productos antivirus eran especialmente buenos detectando malware, pero su uso intensivo de la memoria RAM hacía que las máquinas prácticamente se parasen cuando se lanzaba un análisis. Tras varios batacazos en las pruebas comparativas frente a antivirus que ni hacían uso de la memoria ni detectaban prácticamente nada, se abandonó la idea de hacer estos análisis tan intensos y surgieron productos específicos para esta tarea - se denominaron antimalware y había que lanzarlos manualmente asumiendo que la máquina prácticamente dejaría de responder - separados del producto clásico que se ejecuta de manera continua y analiza casi exclusivamente las imágenes en disco de los archivos.

³¹ En general con señuelos especialmente vigilados y/o marcas de infección conocida que hacen pensar al malware que ya ha infectado un sistema.

³² Aunque las bases de datos son las mismas, generalmente el motor de detección es diferente.

permisos de sistema que ostentan. Sin embargo los recursos de la maquina se ven rápidamente comprometidos y no es eficiente la instalación de más de un producto en local. Además, como la competencia es más feroz el modelo de negocio está migrando a un motor ligerísimo en local que a la más mínima sospecha cifra y empaqueta el archivo para enviarlo a la nube del fabricante y que sea examinado exhaustivamente.

Este comportamiento, si bien es ideal en un entorno doméstico, está absolutamente prohibido en una red acreditada. Podríamos suponer que, por ejemplo, el motor marcarse como sospechoso un documento con información confidencial de nuestra organización y se lo llevase a la nube. Si fuese un falso positivo lo más probable es que se desechase, pero si fuese un archivo legítimo *weaponizado*³³, nuestro archivo real sería compartido entre todos los analistas de malware que trabajan obteniendo y afinando firmas.

Otro de los beneficios de llevar sus análisis a la nube es, en el fondo, similar a nuestro objetivo en donde la “sabiduría colectiva” de cientos de motores livianos en local sospechando de un mismo archivo que está apareciendo en cientos de máquinas por el planeta, puede ser indicativo de una campaña maliciosa en curso. En la imagen siguiente se representan máquinas de usuarios domésticos que en distintos países están detectando un mismo archivo que no saben identificar pero que su *scoring* sugiere una amenaza. Tras su envío a la nube corporativa del fabricante todos los usuarios del antivirus reciben una firma que previene su infección, menos los iniciales que, generalmente, se dan por perdidos.



Figura 5 – Detección híbrida de virus en nube. Fuente: Elaboración propia.

3.3.2 HIDS y NIDS como métodos de detección y alerta temprana.

En las redes acreditadas también se implementan sistemas de detección de intrusiones en curso tanto a nivel de *host* como de red por imperativo normativo [23]. Son los sistemas IDS (*Intrusion Detection Systems* por sus siglas en inglés) que se subdividen en los HIDS

³³ Archivo legítimo en el que se inserta un malware para provocar su ejecución con los mismos permisos en el sistema que tenga el usuario que los activa.

(host IDS) y NIDS (network IDS). Los NIDS se ocupan de los datos transmitidos de un host a otro, mientras que los HIDS se ocupan del análisis de eventos que ocurren en los dispositivos (generalmente a nivel de usuario).

Por lo general los NIDS comparan el paquete con una firma de tipo hash para detectar amenazas, exactamente igual que hacen los antivirus tradicionales, pero en paquetes de red [24]. Cabe destacar que por lo general no implementan ningún tipo de motor heurístico en tiempo real pues podrían provocar retrasos excesivos en la transmisión de paquetes³⁴.

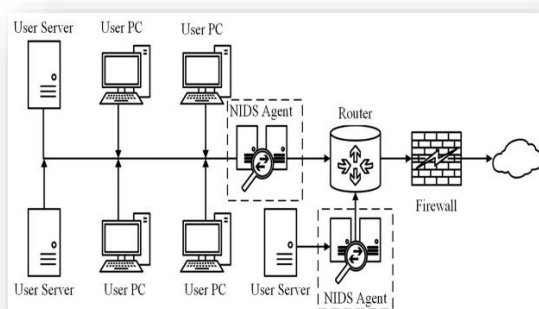


Figura 6 - Agentes NIDS en elementos de red. Fuente: Pro Resources Technology

Por otro lado, los HIDS utilizan diversas técnicas como análisis de registros y logs, verificación de la integridad de los archivos e inspección de artefactos en memoria y del tráfico de red a nivel de sockets en memoria para detectar actividad maliciosa [25]. Al igual que los detectores de red, estos tampoco suelen incorporar técnicas heurísticas, porque por lo general ralentizan los sistemas y los usuarios son muy sensibles a este tipo de retrasos en sus dispositivos.

³⁴ En ciertos dispositivos de red de última generación se realiza DPI (*Deep Packet Inspection*) incluso rompiendo los certificados SSL con técnicas similares a los ataques *Man in the Middle* en copias de los paquetes originales, pero siguen siendo detecciones basadas en firmas y no motores heurísticos.

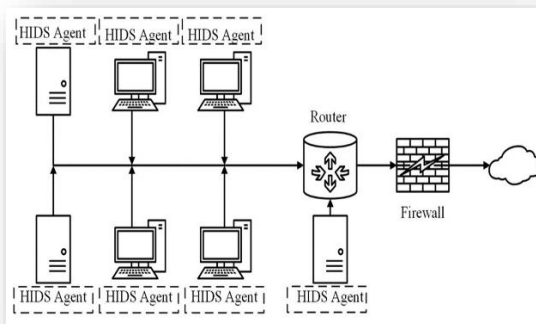


Figura 7 - Agentes HIDS en servidores y endpoints. Fuente: Pro Resources Technology

Los IDS y los antivirus son, por tanto, sistemas complementarios³⁵ que alertan desde diferentes puntos de vista de posibles amenazas. Durante el presente trabajo y concretamente en el capítulo de la **¡Error! No se encuentra el origen de la referencia.** se presenta un método para incluir las alertas humanas que la red de trabajadores ya es capaz de detectar incluso antes de que los sensores software tengan las firmas que los identifiquen como maliciosos.

Esta red de sensores humanos, los trabajadores que ya forman parte de nuestras Fuerzas Armadas, no tiene un modo fácil de alertar de las posibles amenazas que se encuentran en su trabajo diario y su capacidad de raciocinio distribuido, a semejanza del cómputo distribuido, se está desaprovechando.

3.4 Sistemas de Información y Gestión de Eventos de Seguridad

Al profundizar en la operación segura de un sistema y en la seguridad de este, nos encontramos con una familia de herramientas clave, la de los Sistemas de Información y Gestión de Eventos de Seguridad. Estas herramientas son comúnmente conocidas como SIEM y en los últimos años han ido evolucionando e incorporando funcionalidades. Cuando esto ocurre se denominan XDR (por sus siglas en inglés: *Extended Detection and Response*). Estas tecnologías son esenciales para un Centro de Operaciones de Seguridad (COS), actuando como el centro de recopilación de todas las alertas y eventos que ocurren a lo largo de las redes.

El SIEM, en sentido estricto, se dedica a recopilar y analizar registros de eventos de sistemas, aplicaciones y dispositivos en tiempo real. Se trata de una especie de correlador de eventos de distintas fuentes que rastreando patrones y anomalías lanza advertencias sobre posibles amenazas. Desde la monitorización de accesos no autorizados hasta la identificación de comportamientos sospechosos, el SIEM es el cuadro de mando que alerta al COS sobre posibles incidentes de seguridad. Además, el SIEM también facilita

³⁵ Aún aquellos que se publicitan como motores heurísticos capaces de detectar amenazas desconocidas, la realidad es que este tipo de detecciones no es fiable cuando se enfrentan a amenazas programadas específicamente contra una red corporativa como la del MDEF (APT).

la generación de informes y el cumplimiento normativo, lo que contribuye a la transparencia y rendición de cuentas.

El XDR, es una evolución del anterior y la Detección y Respuesta Extendida no se limita a la lectura de logs, sino que incluye la caza proactiva de amenazas [4]. Su enfoque extendido no solo detecta amenazas conocidas, sino que también intenta descubrir nuevas gracias a la identificación de patrones más complejos o desconocidos intentando ofrecer una respuesta más robusta. Además, puede lanzar respuestas automatizadas y ejecutar comandos en remoto, permitiendo al COS actuar rápidamente ante posibles amenazas.

El gran problema de estas soluciones es que hoy en día y para poder dar una respuesta mejor que la de los productos comerciales competidores están migrando a servicios en nube en los centros de proceso de datos de los fabricantes. Con ello pretenden migrar sus soluciones a un modelo de servicios donde proporcionar una capacidad de cómputo gigante sin tener que desplegar soluciones enormes en los clientes, externalizar los mantenimientos de estos hardware, pero, sobre todo, cruzar amenazas entre sus clientes y venderles de nuevo estos resultados como inteligencia corporativa.

Cuando el activo a proteger es una red acreditada el enfoque de un servicio en una nube de un fabricante externo es imposible de implementar. O bien nos conformamos con un SIEM clásico o bien montamos una infraestructura propia de XDR con inteligencia artificial en nuestra nube privada. De ser esta la solución elegida, habría que plantearse la creación de un único proveedor a nivel estatal y para toda la administración de este servicio, de manera que se pudiese mantener la acreditación de las redes monitorizadas y, al igual que las compañías privadas, poder cruzar ataques, patrones y amenazas que ya han comprometido una red para prevenir al resto.

3.5 Cuadro comparativo de soluciones corporativas y sus fortalezas

Para finalizar este capítulo se ha decidido exponer en un cuadro comparativo algunas de las fortalezas y de las debilidades de cada familia de herramientas que se pueden implementar en una red a proteger. Para la comparativa se evalúan los puntos que nos parecen más importantes en criterios de usabilidad, mantenimiento y efectividad de las soluciones que se explican a continuación

P1. Detección de Amenazas: ¿Ofrece una detección proactiva de amenazas sin depender únicamente de firmas conocidas? (SI/NO)

P2. Inteligencia Artificial (IA): ¿Incorpora capacidades de inteligencia artificial para el reconocimiento y adaptación a nuevas amenazas? (SI/NO)

P3. Usabilidad: ¿Es la herramienta fácil de usar para el personal no técnico? (SI/NO)

P4. Impacto en el Rendimiento del Sistema: ¿La herramienta tiene un impacto significativo en el rendimiento del sistema? (SI/NO) – La respuesta SI implica negatividad.

P5. Escalabilidad: ¿Es fácilmente escalable para adaptarse al crecimiento de la red y el volumen de datos? (SI/NO)

P6. Efectividad en Redes Aisladas: ¿Es eficaz en entornos de redes aisladas, sin acceso a actualizaciones frecuentes? (SI/NO)

P7. Colaboración Multifabricante: ¿Puede integrarse fácilmente con soluciones de otros fabricantes para una protección más completa? (SI/NO)

P8. Interfaz de Usuario: ¿La interfaz de usuario facilita la comprensión de los informes y la toma de decisiones incluso para usuarios no técnicos? (SI/NO)

P9. Actualizaciones Automáticas: ¿La herramienta se actualiza automáticamente con las últimas firmas y defensas? (SI/NO)

P10. Costo Total de Propiedad (TCO): ¿El costo de adquisición y mantenimiento es razonable en comparación con su eficacia? (SI/NO)

En el cuadro se incluye una de las herramientas adoptadas por el Centro Criptológico Nacional, Clara, que no se ha tratado durante el capítulo por ser estrictamente un software que comprueba el grado de cumplimiento normativo de la securización de los equipos con respecto a las guías que el CCN promulga. Otras herramientas CCN como Carmen o Claudia se recogen en el siguiente cuadro englobadas dentro de la familia SIEM/XDR y como HIDS respectivamente. ADA es una herramienta parecida a la Plataforma que proponemos, pero su actualización no es automática y esta pensada y dimensionada para su uso por parte del personal de un COS exclusivamente y en ningún caso diseñada para su uso con documentos clasificados. En la última fila se encuentran las fortalezas y debilidades de la Plataforma de análisis Controlado de amenazas que se desarrolla en el Capítulo 4 - **¡Error! No se encuentra el origen de la referencia.**

Tabla 1 – Comparativa de familias de herramientas frente a los criterios de evaluación seleccionados

Redes acreditadas y aisladas	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10
Antivirus local			x	x	x					x
HIDS			x	x	x					x
NIDS			x	x	x					x
SIEM/XDR	x	x					x			x
ADA	x	x			x	x	x	x		x
Plataforma de Análisis Controlado de Amenazas	x		x		x	x	x	x	x	x

Ninguna de las herramientas valoradas cumple la totalidad del espectro. Como ya se ha dicho y repetido a lo largo del trabajo, todas las herramientas son necesarias y cubren la protección del sistema desde diferentes perspectivas en lo que se denomina seguridad en capas. Claramente la generación y puesta en marcha de la Plataforma propuesta aporta una capa extra de protección e incluso cubre aspectos que otras no hacen, como la actualización automática de firmas de detección y la incorporación de las últimas versiones de los motores analíticos comerciales sin interacción humana sujeta a errores.

4. PROPUESTA ALTERNATIVA

El sistema propuesto se basa en una infraestructura de máquinas virtuales, cada una equipada con un software antivirus comercial de un fabricante distinto. Este enfoque aprovecha la multitud de analistas de malware de diferentes compañías trabajando de manera distribuida en nuestro beneficio. La eficiencia no solo radica en la capacidad de estos equipos de analistas diferentes para generar firmas y detectar malware a través de motores comerciales con reglas diversas, sino que también hace uso de la perspicacia de nuestros trabajadores a la hora de detectar anomalías y archivos sospechosos en sus entornos de trabajo digitales. Además, la inclusión de un motor basado en reglas YARA, como el propuesto en el punto 2.1.2 Análisis forense, de generación interna elimina la necesidad de depender exclusivamente de soluciones comerciales y de sus tiempos de respuesta. Asimismo, evitamos el compartir con otras organizaciones de manera incontrolada las vulnerabilidades de nuestros sistemas y aprovechando el conocimiento colectivo de expertos en seguridad.

Todo el proceso debe adherirse rigurosamente a los estándares de seguridad y privacidad establecidos por la organización, así como a la normativa aplicable cuando las redes aisladas están acreditadas para el manejo de información clasificada militar nacional o de alguna de las alianzas de defensa a las que estamos adheridos. Para ello se da por hecho que todas las guías de bastionado relativas a cada una de las tecnologías escogidas se van a aplicar y el sistema al completo se va a someter a un proceso de acreditación que lo certifique. Este enfoque garantiza la protección de los datos sensibles y asegura la operatividad de la red para el fin con el que se diseñó, permitiendo que el sistema de detección se adapte y evolucione en entornos altamente regulados.

Por último, un componente esencial del sistema es el de recopilación de datos que mide el rendimiento del sistema en términos de detección de amenazas y tiempos de respuesta. Esta información no solo es crítica para evaluar la eficacia del sistema, sino que también alimenta una base de datos central accesible para los analistas de malware

de nuestra organización. De este modo se les ofrece no solo un historial detallado de muestras analizadas, sino que también impulsa la generación de firmas internas mediante un motor antivirus distinto a los comerciales. Con esta estrategia se consolida la inteligencia de amenazas interna de la organización y se habilitan mecanismos capaces de detectar anticipadamente ataques con herramientas nuevas y aún no catalogadas por los productos comerciales.

4.1 Casos de uso

Para esbozar el sistema se ha hecho uso de la metodología de casos de uso y “*user stories*” para el desarrollo de sistemas. De este modo, se proporciona una estructura clara y comprensible para describir las interacciones clave siguiendo el mismo enfoque que se explica en [26] y se aplica en [27].

Dentro de esta terminología, cada caso de uso representa una funcionalidad específica del sistema, un bloque de alto nivel en el que se detallan las acciones de los actores involucrados con los flujos de trabajo que se integran. Esta metodología no sólo simplificará la comunicación entre los equipos de desarrollo y los *stakeholders*, sino que también servirá como una guía esencial para la planificación y ejecución de cada componente del sistema durante sus etapas de desarrollo. Los “*user story*” son más breves y se centran en la funcionalidad desde la perspectiva del usuario, mientras que los “*use case*” tienden a ser más detallados y abordan varios aspectos, incluidos actores, flujo del proceso y posibles extensiones [28].

A continuación, y como primera aproximación a la metodología para el lector inexperto, vamos a describir un “*use case*” simplificado con un enfoque narrativo más cercano a un “*user story*”, en el que vamos a describir todo el sistema propuesto a grandes rasgos. Además se añade en la siguiente imagen un diagrama de casos de uso.

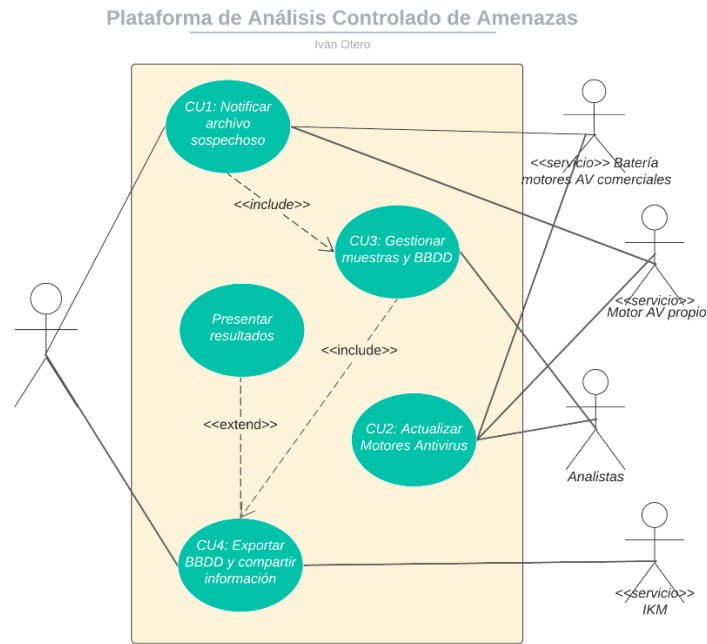


Figura 8 - Diagrama de Casos de Uso. Fuente: Elaboración propia

Caso de Uso: Plataforma de análisis controlado de amenazas en una red Corporativa Aislada

1. Nombre del Caso de Uso:

Análisis de Malware en Red Corporativa Aislada

2. Descripción:

Este caso de uso describe el proceso mediante el cual los usuarios de la red corporativa aislada pueden analizar archivos sospechosos sin conexión a internet, utilizando un sistema multimotor de análisis de malware accesible con menos de 3 clics de ratón desde un equipo corporativo.

3. Actores Involucrados:

- Usuario de la Red Aislada: Personal debidamente autorizado y autenticado que desea analizar archivos sospechosos en una red sin acceso a internet.
- Plataforma de análisis controlado de amenazas: Sistema que integra el análisis de varios motores antivirus para realizar el estudio en un entorno aislado.

4. Flujo del Proceso:

- Inicio del Proceso:
 - El usuario identifica un archivo sospechoso en la red corporativa aislada.
 - Selecciona la opción de análisis y envía el archivo a la plataforma.
- Análisis Multimotor en Entorno Aislado:

- El sistema se encarga de identificar de forma unívoca la muestra (sha256+MD5) y la pone a disposición de ser analizada por todas las plataformas de análisis.
- El sistema comprueba que no se haya realizado un análisis sobre la misma muestra en un período menor a 24 horas tras la actualización de los motores. Si así fuese, mostraría los resultados del análisis anterior y guardaría la información de cuantos usuarios distintos han solicitado un análisis sobre dicha muestra.
- Cada motor antivirus realiza un análisis independiente sin conexión a internet en una máquina virtual desechable tras el análisis que es copia exacta de los equipos clientes de la red corporativa.
- **Recopilación de Resultados:**
 - Los resultados de cada motor antivirus se recopilan y se genera un informe consolidado.
 - Se envía un link al mail corporativo del usuario que inició el proceso para consulta asíncrona.
 - Se identifican las detecciones positivas y negativas de cada motor en el entorno aislado y se asocia con la identificación hash que se creó al principio del flujo.
- **Presentación de Resultados al Usuario:**
 - El informe se presenta al usuario a través de una web en intranet, al finalizar el análisis o al hacer click en un link que se envía a su correo corporativo interno.
 - Se proporciona información sobre la naturaleza del malware detectado, si lo hay.
- **Acciones del Usuario:**
 - El usuario puede tomar decisiones basadas en los resultados como eliminar el archivo si es un malware reconocido y el aviso a la red de procedencia (trazabilidad) de la existencia de un archivo malicioso.
- **Fin del Proceso:**
 - El caso de uso concluye para el usuario cuando ha tomado las acciones necesarias.
 - Si existe un malware se lanza una alerta a los laboratorios forenses y de análisis de malware por si hubiese que emprender más acciones.
 - Por último, las máquinas virtuales utilizadas para el análisis se revierten a su estado inicial. Esto garantiza que la siguiente ejecución del análisis comience con una imagen limpia y actualizada, preparada para nuevos escaneos.

5. Condiciones de Éxito:

- La plataforma analiza eficazmente el archivo sospechoso en un entorno sin conexión a internet.

- Los resultados son presentados de manera clara y comprensible para el usuario en la red corporativa aislada vía intranet.
- Las acciones tomadas por el usuario son efectivas para mitigar las amenazas.
- El personal del COS es informado de la existencia de una amenaza en curso tras un positivo.
- Si un archivo no es detectado como una amenaza por ninguno de los motores, pero se ha solicitado su análisis por más de 3 usuarios distintos en menos de 8 horas o 10 en menos de 7 días se lanzará una alerta al servicio de análisis de malware del COS.

6. Extensiones y Variaciones:

- Análisis Programado:
 - Posibilidad de programar análisis automáticos en momentos específicos para ciertas muestras seleccionadas para comprobar cómo cambian las detecciones de los motores.
- Integración con Sistemas de Seguridad en Red Aislada:
 - Integración de la información obtenida con otros sistemas, de seguridad y de inteligencia, para una respuesta más amplia ante amenazas en el entorno aislado.

A continuación, vamos a ver 4 *use cases* estrictos en los que se describirá cada uno de los grandes componentes del sistema con la intención de clarificar cual es la solución que se intenta aportar con este trabajo y sentar las bases de este futuro sistema de análisis de malware.

4.1.1 Bloque de interacción con el usuario.

El primer caso de uso es el que describe el módulo que interacciona con los trabajadores concienciados de nuestra organización, les dota de un sistema de comunicación de sus sospechas y agrega automáticamente los archivos a su solicitud. Además, es capaz de, en poco tiempo, devolver una evaluación inicial sobre sus sospechas por si fuese un malware conocido y así evitar la infección del sistema de información corporativa.

Caso de Uso: Bloque de interacción con el usuario

1. Nombre del Caso de Uso:

Notificar archivo sospechoso.

2. Descripción:

Este caso de uso describe la parte del sistema que permite a los usuarios de la red corporativa aislada enviar los archivos sospechosos a analizar, así como la presentación de los resultados de manera accesible y comprensible.

3. Actores Involucrados:

- Usuario de la Red: Personal autorizado y autenticado preocupado por la existencia de un archivo potencialmente malicioso.
- Plataforma de Análisis Controlado de Amenazas: Sistema subyacente que ejecuta el análisis de malware y proporciona resultados a la interfaz web.

4. Flujo del Proceso:

- Inicio del Proceso:
 - El usuario sospecha de un archivo, o de la procedencia de este, durante su jornada laboral habiéndose autenticado debidamente en la red.
- Carga y Envío de Archivos:
 - El usuario selecciona la opción de envío para análisis desde una opción del menú emergente que se ofrece con botón derecho en el explorador de la imagen del sistema operativo corporativo al señalar el archivo.
 - El archivo sospechoso se comprime con una contraseña de sesión y se sube a un sistema de ficheros seguro de manera que los antivirus de los elementos de red internos no borren la alerta de origen humano.
 - El usuario recibe confirmación de que el archivo ha sido enviado para su análisis y se le ofrece un link de intranet donde poder visualizar el resultado cuando este completo.
- Presentación de Resultados:
 - La interfaz web muestra el progreso del análisis en tiempo real.
 - Una vez completado el análisis, se presenta un informe consolidado de los resultados.
 - En posición prominente se informará con un código de tres colores (verde, amarillo o rojo) sobre el nivel de peligrosidad de la muestra.
 - Se destaca cualquier detección positiva de malware, proporcionando detalles sobre la naturaleza de la amenaza.
- Notificación al Usuario:
 - Se envía automáticamente un correo al mail corporativo del usuario con un enlace para consultar los resultados más tarde.
- Acciones del Usuario:
 - El usuario revisa los resultados y toma decisiones basadas en la información proporcionada.
 - Si alguno de los motores detecta la muestra como maliciosa se le permitirá al usuario añadir información libre, en formato texto, sobre procedencia del archivo u otros datos que crea importantes.
 - Puede eliminar el archivo si es malicioso y notificar a la red de origen si la conoce y cree que es necesario.
- Fin del Proceso:

- El caso de uso concluye cuando el usuario ha revisado los resultados y ha tomado las acciones necesarias.

5. Condiciones de Éxito:

- La forma de iniciar un análisis es sencilla y solo requiere del uso del ratón en la imagen corporativa del sistema operativo.
- Los resultados del análisis se presentan de manera clara y accesible.
- El usuario recibe notificaciones oportunas y accede fácilmente al informe a través del enlace proporcionado en su correo.
- Toda la presentación web ocurre exclusivamente en intranet.

6. Extensiones y Variaciones:

- Posibilidad de integrar el servicio web con sistemas de seguridad adicionales y mostrar cuadros de mando con información oportuna según el usuario que está accediendo a ellos.
- Mejoras continuas en la usabilidad y diseño de la interfaz para una experiencia del usuario mejorada.

4.1.2 Procedimiento de actualización de motores/Sistema de exclusas.

Para poder asegurar que los análisis se hacen con las últimas detecciones comerciales y privadas disponibles necesitamos dotar al sistema de un módulo de actualización de motores y firmas de manera que, a pesar de acceder a repositorios públicos, generalmente en internet, se mantenga la acreditación de la red donde se usa el sistema.

Caso de Uso: Mantenimiento y Actualización de los Antivirus

1. Nombre del Caso de Uso:

Actualizar Motores Antivirus.

2. Descripción:

Este caso de uso describe el proceso automático que asegura la actualización regular de los motores de antivirus, verificando la disponibilidad de nuevas firmas y software. Esto garantiza que el sistema de análisis de malware esté siempre equipado con las últimas versiones disponibles.

3. Actores Involucrados:

- Sistema Automático de Actualización: El proceso automatizado encargado de mantener actualizados los motores de antivirus.
- Proveedor de Antivirus: El fabricante del software antivirus que proporciona las actualizaciones.

4. Flujo del Proceso:

- Inicio del Proceso:

- El sistema automático se activa diariamente a las 4 de la mañana.
- **Conexión a Internet y Actualización:**
 - Se levanta una imagen corporativa con un motor de antivirus instalado.
 - La imagen virtual se conecta a internet exclusivamente a través de una conexión segura y controlada.
 - Se accede únicamente al servicio de actualización de firmas y motores del fabricante de antivirus quedando explícitamente excluidas cualquier conexión a otro servidor distinto.
 - Las consultas DNS, si fuesen precisas, se harán al proveedor corporativo interno en DMZ y nunca directamente a un proveedor externo.
 - Se verificará la disponibilidad de nuevas versiones de firmas o del software del motor.
 - En caso de actualizaciones, se descargan e instalan.
- **Pausa y Clonación:**
 - La imagen virtual se pone en pausa después de la actualización.
 - Se clona la imagen actualizada para su posterior distribución en la red interna.
- **Transferencia a la Red Interna:**
 - A través de un sistema de esclusas, se copia la imagen clonada a la parte interna de la red aislada.
 - Se utiliza una DMZ de intercambio dentro/fuera con dos firewalls, uno a cada lado y de distintos fabricantes, para asegurar un proceso de transferencia seguro y la rotura del protocolo de red.
 - Se descarta cualquier archivo no autorizado en la DMZ, esto es imagen virtual de la máquina, y se alerta al personal del COS.
- **Fin del proceso:**
 - Tras recibir una máquina con una versión nueva de un fabricante se arrancará con un archivo de prueba para confirmar que la instalación ha sido correcta y las detecciones siguen funcionando e informando correctamente.
 - Si las comprobaciones son exitosas, se borra la máquina antigua para ese fabricante específico y se enlazarla la máquina con el servidor seguro de ficheros para entrar en producción cuando haya una nueva muestra.
 - Se genera un informe para los administradores del sistema con las posibles incidencias y las verificaciones llevadas a cabo para cada fabricante.

5. Condiciones de Éxito:

- Todas las actualizaciones se han verificado y aplicado correctamente.

- Cada imagen clonada se ha transferido de manera segura a la red interna.
- La DMZ de intercambio dentro/fuera solo contiene archivos autorizados para el análisis de malware.

6. Extensiones y Variaciones:

- Posibilidad de programar actualizaciones adicionales si es necesario para campañas en curso o fabricantes muy prolíficos.
- Mejoras continuas en la seguridad del proceso de transferencia y en las actualizaciones de los sistemas de protección perimetral de la DMZ siempre con las recomendaciones de la entidad certificadora.

4.1.3 *Backend*

En este bloque se describe a través de un caso de uso las funcionalidades que aporta este sistema como elemento de alerta a nuestros equipos de forenses y analistas de malware que trabajan en los diferentes COS de nuestra organización.

Caso de Uso: Acciones en el Backend y Gestión de Muestras Analizadas

1. Nombre del Caso de Uso:

Gestionar muestras y bases de datos

2. Descripción:

Este caso de uso describe el proceso para gestionar las bases de datos internas del sistema en donde se almacena información detallada sobre las muestras analizadas. Desde la prevención de reanálisis innecesarios hasta alertar sobre amenazas potenciales mal catalogadas previamente. Estos procesos y bases de datos son esenciales para la eficacia del sistema.

3. Actores Involucrados:

- Bases de Datos: Sistemas que almacenan y gestionan información detallada sobre las muestras analizadas.
- Analistas de Malware y Forenses: Personal encargado de realizar análisis manuales y tomar acciones basadas en alertas generadas por el sistema.
- Usuarios Iniciales: Personas que han enviado muestras para su análisis.

4. Flujo del Proceso:

- Prevención de Reanálisis:
 - El sistema verifica si una muestra ha sido analizada en un período reciente gracias a su identificación basada en hash.
 - Evita, también, reanalizar muestras gracias al identificador temporal de la última actualización de los motores antivirus.
- Registro de Usuarios y Muestras:

- Cada vez que un usuario envía una muestra, se registra en la base de datos junto con información detallada sobre la muestra, el usuario y una marca temporal.
- Alertas a Analistas y Usuarios:
 - El sistema alerta a los analistas y forenses sobre muestras que podrían contener amenazas no detectadas por los motores de antivirus cuando el número de usuarios o las peticiones de reanálisis superen los umbrales predefinidos.
 - En el caso de una muestra que ha cambiado su evaluación de benigna a maliciosa, el sistema notifica a los usuarios iniciales y a los analistas del cambio.
- Análisis Manual:
 - Las muestras marcadas por el sistema para un análisis manual se envían a los analistas de malware y forenses.
 - Los analistas toman las acciones necesarias, como iniciar una investigación más profunda o tomar medidas correctivas.
- Historial de Muestras:
 - La base de datos mantiene un historial detallado de cada muestra, incluidas las detecciones y acciones tomadas en análisis anteriores.
 - El servidor de ficheros guarda una muestra comprimida con contraseña en una cuarentena segura de cada archivo sospechoso, aunque haya sido marcado como benigno.

5. Condiciones de Éxito:

- La base de datos evita reanalizar muestras innecesariamente.
- Los analistas son alertados sobre posibles amenazas emergentes.
- Los usuarios iniciales son notificados sobre cambios en la clasificación de muestras que habían reportado.
- El historial de muestras proporciona una trazabilidad completa y detallada.

6. Extensiones y Variaciones:

- Posibilidad de agregar información adicional a la base de datos para un análisis más detallado.
- Integración con sistemas de inteligencia de amenazas para una respuesta más rápida a nuevas amenazas.

4.1.4 Detección de APT y otras amenazas específicas contra nuestros intereses.

Gracias a la red de usuarios concienciados podremos, idealmente, identificar las primeras etapas de un ataque APT o de otro tipo que aún son capaces de evitar las detecciones de los antivirus comerciales y que se marcan para un análisis manual por nuestros analistas debido a la acumulación de envíos para su análisis por parte de nuestros trabajadores. En este caso de uso se va más allá de lo obvio y se esboza el módulo capaz

de exportar la inteligencia corporativa a otras redes clasificadas de nuestro ministerio o de otros organismos de la Administración General del Estado que adopten e implanten esta solución.

Caso de Uso: Exportación de Bases de Datos de Amenazas en Curso y Motor Antivirus Propio

1. Nombre del Caso de Uso:

Exportar bases de datos y compartir información

2. Descripción:

Este caso de uso se enfoca en la posibilidad de exportar las bases de datos de malware detectadas en cualquiera de nuestras redes aisladas para alimentar el resto de los sistemas gemelos instalados en las demás redes, incluyendo un motor antivirus propio de la organización basado en firmas YARA. Este motor privado permite detectar amenazas que los antivirus comerciales podrían pasar por alto.

3. Actores Involucrados:

- Bases de Datos: Sistemas que almacenan y gestionan información detallada sobre las muestras analizadas.
- Motor Antivirus Propio: Motor de análisis basado en firmas YARA, desarrolladas internamente por nuestros analistas de malware.

4. Flujo del Proceso:

- Generación del Motor Antivirus Propio:
 - Los analistas de malware generan firmas YARA para amenazas que los antivirus comerciales no detectan, pero que la organización ha identificado como maliciosas.
 - Estas firmas se incorporan al motor antivirus propio de la organización.
- Exportación de Bases de Datos:
 - Se establece un sistema automatizado para exportar bases de datos de malware detectadas, incluyendo detecciones del motor antivirus propio.
 - Las bases de datos exportadas se utilizan para alimentar sistemas multimotor en otras redes aisladas.

5. Condiciones de Éxito:

- Las firmas YARA generadas por los analistas se integran con éxito en el motor antivirus propio.
- El motor antivirus propio detecta amenazas según las firmas YARA y se actualiza con detecciones positivas de amenazas materializadas en otros sistemas corporativos.
- Las bases de datos se exportan de manera eficiente y segura a través de un repositorio en la DMZ de actualización de máquinas virtuales.

- Las plataformas de análisis controlado de amenazas en otras redes se actualizan con las detecciones más recientes, incluyendo las del motor antivirus propio.

6. Extensiones y Variaciones:

- Posibilidad de lanzar un análisis con las nuevas firmas YARA a archivos que anteriormente se habían catalogado como inocuos pero que siguen en nuestra cuarentena.
 - Integración con sistemas de gestión centralizada para coordinar la exportación y difusión de las bases de datos de amenazas en curso.

4.2 Tecnologías escogidas para el sistema final

Para finalizar este capítulo se sugieren algunas de las posibles tecnologías clave que respaldarán la estructura propuesta. En el núcleo de la plataforma de análisis automático de malware, vSphere³⁶ actuará como el software de virtualización principal, aprovechando EXSi para ejecutar máquinas virtuales que albergarán los motores antivirus, y vCenter para orquestar actualizaciones y la gestión dinámica de estas máquinas. La elección de vSphere se basa en su liderazgo en el mercado, su robustez y eficiencia, y la familiaridad de nuestro personal con esta tecnología.

A nivel de servidores, Windows Server se posiciona como el sistema operativo principal, respaldado por su capacidad para gestionar diversas funciones y servicios, mientras que Windows 10 se implementará en cada endpoint virtualizado, replicando fielmente el entorno tecnológico a proteger. Esta elección se guía tanto por su presencia cotidiana en nuestra organización como por su capacidad para reflejar de manera precisa la superficie de ataque.

La seguridad del sistema se fortalecerá mediante el uso de diodos certificados³⁷, actuando como guardianes para prevenir flujos no deseados de información. Este enfoque es vital para preservar la integridad del sistema y garantizar que la información sensible circule solo en las direcciones autorizadas.

La gestión de información y resultados de análisis se confiará a MongoDB, una base de datos relacional reconocida por su eficiencia y escalabilidad en el manejo de grandes

³⁶ En el presente documento se habla de vSphere por ser la solución corporativa actual del MDEF y con la que tenemos más experiencia. El sistema propuesto no depende de la solución de virtualización y sería fácilmente exportable a otras tecnologías como HyperV, que también están presentes en nuestra organización, pero con una penetración menor.

³⁷ En España, existe una guía preaprobada de productos que cumplen las especificaciones técnicas necesarias para el manejo de documentación clasificada. Es la guía CCN-STIC 105, de acceso público, y en ella se listan todos los diodos y pasarelas que servirían para este propósito.

volúmenes de datos, esencial para recopilar y almacenar los resultados del análisis de las muestras.

Power BI Server entrará en juego para la presentación de datos, generación de cuadros de mando y la toma de decisiones. Esta herramienta facilita la creación de cuadros de mando visuales e interactivos, permitiendo a los analistas interpretar rápidamente la información.

La creación del motor antivirus propio se llevará a cabo con Yara, una herramienta versátil para la generación de firmas y detección de malware, potenciando la capacidad del sistema para enfrentar amenazas conocidas y desconocidas.

La flexibilidad de la plataforma es una de sus características más destacables. Las tecnologías mencionadas no son estáticas, permitiendo la adaptación y sustitución según las necesidades específicas del sistema a proteger o acuerdos corporativos y un cambio relativamente rápido a otros productos como pudiesen ser Hyper-V o bases de datos Oracle. Por tanto, la plataforma se presenta, de cara a las redes a proteger, como un servicio adaptable a diferentes contextos tecnológicos, proporcionando una capa adicional de defensa contra comportamientos anómalos mediante el uso estratégico de tecnologías líderes, siempre que puedan ser debidamente acreditadas.

5. CONCLUSIONES, NUEVAS LÍNEAS DE TRABAJO Y OTROS USOS POSIBLES

En el complejo universo de la ciberseguridad, en relación con el malware, se puede afirmar que las amenazas APT se erigen como maestras del camuflaje, eludiendo incluso a los más avanzados sistemas antivirus comerciales que solo los identifican por patrones binarios o de comportamiento. Su programación y sus técnicas evasivas les permiten mimetizarse durante largos períodos, infiltrándose sigilosamente en el tejido digital de las organizaciones adversarias. Por si no fuese suficiente, la aparición de tecnologías disruptivas, como la inteligencia artificial, el Internet de las Cosas (IoT) y la computación cuántica, han supuesto un desafío adicional para los ciberdefensores. Aunque estos avances ofrecen innumerables beneficios, también abren puertas a nuevas vulnerabilidades que los ciberdelincuentes pueden explotar. La protección frente a estas amenazas emergentes requiere cada vez más de un enfoque proactivo, combinando la innovación tecnológica con sólidos principios de seguridad.

La resistencia ante los continuos ataques requiere cada vez más de un profundo compromiso de los usuarios y operadores de sistemas de la propia institución y no solo en la inversión en barreras tecnológicas. Es por lo que la inversión en la concienciación, formación continua y la generación de la cultura de trabajo basada en principios seguridad está dejando de ser una opción para convertirse en una obligación de cualquier institución para la que la seguridad sea un pilar fundamental.

Durante años se ha dado por cierto que el factor humano es una debilidad de los sistemas de información y, sin ser totalmente falso, se constata que es necesario cambiar este marco mental y convertirlo en nuestra primera línea de defensa dotándolo de herramientas y conocimientos que lo conviertan en una fortaleza. La ciberseguridad debe nutrirse de la vigilancia y el conocimiento de quienes interactúan con los sistemas y los conocen hasta el nivel de detectar pequeñas anomalías. La formación constante y la conciencia de las tácticas empleadas por los adversarios son pilares fundamentales para blindar las redes contra intrusiones no deseadas, sobre todo, cuando estas redes son vitales para los intereses de organizaciones al servicio de las naciones.

En entornos militares, donde la seguridad de la información reviste una importancia crítica, el liderazgo efectivo es también un componente clave. La toma de decisiones ágil y la implementación de estrategias basada en datos veraces y confiables son esenciales para salvaguardar las redes en un contexto donde los riesgos son especialmente elevados. En las grandes redes corporativas, la recopilación, el análisis constante y la fusión de datos de cientos de sensores para generar inteligencia basada en ellos no solo sirven para identificar amenazas potenciales, sino que también contribuyen a trazar patrones y tendencias que permiten reforzar las defensas establecidas inicialmente a la hora de crear un sistema de información y analizar sus riesgos potenciales.

El análisis de riesgos, previo incluso a la creación, de un sistema de información se convierte en la piedra angular de la seguridad. La evaluación meticulosa de activos, vulnerabilidades y amenazas proporciona una base sólida para la implementación de salvaguardias y estrategias de mitigación. La seguridad no es un estado estático, y la revisión y actualización periódica del análisis garantiza la adaptabilidad continua del sistema frente a los cambios constantes de los intereses de las amenazas externas.

La acreditación de estas redes, respaldada por un estricto control de acceso, proporciona un nivel adicional de seguridad que permite el manejo y la custodia de información con clasificación de seguridad. Estos entornos altamente securizados se erigen como bastiones digitales, donde el acceso está reservado a aquellos con autorización explícita y la necesidad de conocer. Este enfoque no sólo protege contra amenazas externas, sino que también mitiga riesgos internos. Sin embargo, la historia demuestra que pese a todas las medidas que se puedan implementar, si una nación está decidida a conocer los secretos de otra, acabará accediendo a ellos. Para evitarlo, o al menos retrasarlo, las redes acreditadas incorporan herramientas avanzadas, como señuelos y sistemas de monitorización. Estos servicios desempeñan un papel vital en la identificación temprana de patrones de ataque gracias a la creación de cebos digitales y la observación continua de la red, permitiendo a los equipos de seguridad anticipar movimientos hostiles y fortalecer las defensas antes de que desemboquen en ataques completos.

En la constante competición entre defensores y atacantes, los programas antivirus son una ayuda importante para los primeros, pero necesitan evolucionar constantemente. Estas herramientas se ajustan y actualizan para hacer frente a las tácticas, técnicas y procedimientos de los atacantes que, de la misma manera, no dejan de cambiar y adaptarse para intentar pasar desapercibidos. Sin bien, para los atacantes es realmente sencillo que su malware se esconda de alguno de estos motores comerciales, se puede afirmar que no lo es tanto evitarlos a todos a la vez. Las mejoras constantes en su eficiencia y detección y la alta competitividad del mercado hacen que cada solución enfrente las adaptaciones de las amenazas de manera diferente y con una frecuencia diaria muy difícil de mantener en el tiempo para los programadores de malware.

La creación del sistema que hemos esbozado a través de casos de uso representa un paso adelante en la evolución de las estrategias de ciberdefensa en entornos aislados. La

implementación de un análisis multimotor, con soluciones antivirus de fabricantes diferentes, permite una defensa proactiva y robusta contra amenazas conocidas y emergentes. Este enfoque diversificado no solo capitaliza los esfuerzos y los conocimientos de diversos fabricantes, sino que también minimiza la debilidad que supone la dependencia de una única solución comercial. Por otra parte, la red de sensores humanos distribuidos en toda la infraestructura agrega una capa adicional de vigilancia y detección inédita hasta la fecha y que capitaliza las inversiones en formación y concienciación de la organización. Al aprovechar la capacidad de razonamiento distribuido de los empleados, se transforman en nodos activos en la red de sensores de detección temprana de amenazas. Además, debido a la alta modularidad del sistema debemos señalar como característica intrínseca al mismo su extensibilidad y su bajo coste en tiempo y recursos económicos para adaptarlo a nuevas características o actualizar sus funcionalidades.

La generación de un motor antivirus propio, basado en firmas YARA de amenazas conocidas, pero no detectadas por soluciones comerciales, marca también un hecho diferencial en la aplicación directa e inmediata de la inteligencia corporativa. Este motor, alimentado por los resultados obtenidos por nuestros analistas de malware, agrega una capa adicional de análisis, identificando amenazas que podrían haber eludido el resto de las capas de seguridad implementadas.

En conjunto, el sistema propuesto no solo cumple con los estándares de seguridad y privacidad, sino que transforma el capital humano de la organización en una fortaleza capitalizando la inteligencia colectiva de nuestro personal y alertando sobre archivos sospechosos que han logrado superar las barreras. El triaje al que se somete a estos archivos en la batería multimotor evitará horas de análisis vacuos y la fuga inadvertida de información si se consultase con servicios online que proporcionan funcionalidades parecidas. La monitorización continua, la rápida respuesta a incidentes y la generación interna de reglas y firmas aseguran un enfoque completo y robusto contra las amenazas digitales actuales. Este sistema es, por tanto, una de las respuestas posibles a la complejidad creciente del ciberespacio, donde la innovación, la colaboración y la suma de la inteligencia colectiva se convierten en las claves para mantener la integridad de la infraestructura digital corporativa y de la documentación que contiene.

Con este trabajo se ha pretendido sentar las bases de la creación de un sistema robusto, aislado de redes de terceros, que aproveche la alta preparación de nuestro personal para detectar software malicioso que pueda suponer un peligro para nuestras redes. Se procuraba, en definitiva, señalar una manera posible de evitar los riesgos derivados del hecho de que los productos antivirus actuales y otras herramientas de seguridad tienden a transformarse en servicios en nube. Estas nubes, que no son privadas y exclusivas, aprovechan las detecciones de sus softwares en centenas de miles de *endpoints* que, a modo de sensores distribuidos, envían al fabricante alertas que sirven para generar lo que se conoce como inteligencia de la amenaza. Además, y como un añadido a la solución apuntada se deja de depender de la inteligencia de un único fabricante para aglutinar las detecciones y el conocimiento de múltiples analistas y sus soluciones.

A partir de este trabajo surgen varias líneas de estudio para otros o ampliaciones de los casos de uso del presente sistema. Por ejemplo, la implementación de servicios y *appliances* de *sandboxing* añadirían valor a los resultados del sistema, pero no suponen más que una mejora en los análisis y no merecen un estudio en profundidad. Expondremos, por tanto, algunas líneas de las que sí nos parecen más inmediatas, útiles y efectivas para implementar una vez que el sistema base ya esté funcionando.

El uso posible con más espíritu militar no podía ser otro que el de la evaluación de las mitigaciones, defensas y sensores de nuestra red a la vez que utilizamos la misma tecnología para probar las armas software propias contra baterías de motores heurísticos, firmas actualizadas y personal concienciado. Este enfoque permitiría una comprensión más profunda de las vulnerabilidades potenciales de los sistemas clasificados y una mejora continua en las tácticas de evasión de los motores comerciales para el personal militar encargado de las operaciones ofensivas en este dominio.

Otra línea de investigación, extensión de la presentada en este trabajo, debería centrarse en la creación de un servicio basado en la instalación de una pieza software corporativa en todos los dispositivos de usuario de la red. Este programa, con privilegios suficientes, será capaz de examinar todos los archivos y artefactos de un endpoint en busca de una amenaza específica para la cual hemos generado una firma yara interna. Este servicio reportaría directamente al personal del COS de sus hallazgos y sería una forma de aprovechar la potencia de computación distribuida de nuestras redes a la hora de localizar más infecciones de amenazas que los antivirus tradicionales todavía no conocen.

Para finalizar nos gustaría señalar que si este sistema se muestra tan efectivo como presuponemos, debería ser compartido, de manera que la colaboración y el intercambio de recursos sean el eje de la propuesta de ofrecer la Plataforma de Análisis Controlado de Amenazas como servicio para todas las redes de la Administración General del Estado. El verificar que tipo de información buscan nuestros adversarios en otros departamentos ministeriales y el hecho de poder extender la búsqueda basada en firmas YARA de generación propia podría producir sinergias significativas, fortaleciendo las defensas colectivas y estableciendo un estándar elevado de seguridad en toda la administración.

Gracias a la generación del sistema base e implementado todas estas líneas de trabajo futuras no solo se profundizaría en la robustez del sistema propuesto, sino que también se abre la puerta a contribuciones significativas y a la comprensión de la ciberseguridad como una necesidad conjunta de todos los ministerios y sus organismos dependientes. De esta manera se llegaría a consolidar el sistema no solo como una herramienta efectiva sino como una plataforma innovadora y colaborativa, a todos los niveles, en la defensa contra amenazas digitales en constante evolución.

6. BIBLIOGRAFÍA

- [1] Accenture, «Cyber Threat Intelligence and Trends Report,» 15 febrero 2022.
- [2] K. A. Monnappa, Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware., Birmingham: Packt, 2018.
- [3] M. Guerra Soto, Análisis de malware para sistemas Windows., Madrid: Ra-Ma, Ed, 2018, p. 554.
- [4] M. Guerra Soto, Ciberinteligencia de la amenaza en entornos corporativos, Ra-Ma, Ed., Paracuellos del Jarama, Madrid: Ra-Ma, 2023.
- [5] Interpol, «Análisis forense digital,» [En línea]. Disponible: <https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital>. [Último acceso: 11 noviembre 2023].
- [6] D. F. J. López Cánovas y D. C. Chiclana, «Engagement, una plataforma para el desarrollo de la persona.,» *Comunicación Y Hombre*, nº 14, pp. 55-64, 2018.
- [7] . García, Cero Accidentes: El Sistema de Seguridad Preventiva Total: Cero Accidentes y Cero Paradas en la Producción Por Accidentes, Amazon Digital Services LLC - KDP Print US, 2020, p. 408.
- [8] A. Allueva Pinilla y J. L. Alejandro Marco, Enfoques y experiencias de innovación educativa con TIC en educación superior, Zaragoza: Prensas Universitarias de Zaragoza, 2019, p. 334.

- [9] A. L. Barnhill, *Train as You Will Fight, Factors Affecting Development of a Strategy to Train National Guard Units to the Level Organized*, Fort Leavenworth: U.S. Army Command and General Staff College, 1990.
- [10] Zippia, «25 Gamification statistics [2023]: Facts + Trends you need to know,» 23 febrero 2023. [En línea]. Disponible: <https://www.zippia.com/advice/gamification-statistics/>.
- [11] M. O. Gómez, *En busca de un modelo de resiliencia cibernética basado en las experiencias de la OTAN*, Buenos Aires: Editorial Autores de Argentina, 2019.
- [12] Dirección General de Modernización Administrativa, *Procedimientos e Impulso de la Administración Electrónica, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.*, Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.
- [13] F. J. Gamboa Herráiz, «La OTAN más allá de la Resiliencia,» *Documento de Opinión 93/2023*, p. 13, 3 noviembre 2023.
- [14] S. Fagerland y W. Grange, «The Inception Framework: Cloud-hosted APT,» Blue Coat Systems, Inc, 2015.
- [15] Flexa, «Threat Intelligence: ¿Cuáles son los beneficios de esta estrategia?,» [En línea]. Disponible: <https://flexa.cloud/es/beneficios-de-la-inteligencia-de-amenazas/>. [Último acceso: 11 noviembre 2023].
- [16] Energy5, «El papel del intercambio de inteligencia sobre amenazas en la ciberseguridad de la respuesta a la demanda,» [En línea]. Disponible: <https://energy5.com/es/el-papel-del-intercambio-de-inteligencia-sobre-amenazas-en-la-ciberseguridad-de-la-respuesta-a-la-demanda>. [Último acceso: 11 noviembre 2023].
- [17] J. Oltsik, «Los programas de inteligencia de amenazas, preparados para crecer,» 12 junio 2023. [En línea]. Disponible: <https://cso.computerworld.es/tendencias/los-programas-de-inteligencia-de-amenazas-preparados-para-crecer>. [Último acceso: 11 noviembre 2023].
- [18] Kaspersky Labs, «¿Qué es la inteligencia de amenazas? Definición y explicación,» [En línea]. Disponible: <https://latam.kaspersky.com/resource-center/definitions/threat-intelligence>. [Último acceso: 11 noviembre 2023].
- [19] Tenable, «Cómo volverse un líder de seguridad alineado con el negocio,» 1 enero 2020. [En línea]. Disponible: <https://es-la.tenable.com/ebook/how-to-become-a-business-aligned-security-leader>. [Último acceso: 11 noviembre 2023].

- [20] J. C. e. a. Liporace, «Metodología para el análisis de incidentes de ciberseguridad o ciberataques durante las acciones de ciberdefensa de las infraestructuras críticas de la defensa nacional,» de *XXI Workshop de Investigadores en Ciencias de la Computación*, Puerto Rico, 2019.
- [21] Centro Criptológico Nacional, «Procedimiento de Seguridad de las TIC - CCN-STIC 101,» Ministerio de la Presidencia y para las Administraciones Territoriales, Madrid, 2016.
- [22] A. Corletti Estrada, *Seguridad por niveles*, DarFE, 2011.
- [23] Centro Criptológico Nacional, «Herramientas de Seguridad en el ENS - CCN-STIC 818,» Centro Criptológico Nacional, Madrid, 2012.
- [24] A. Ali Shah, M. Sikander Hayat y M. Daud Awan, «Analysis of Machine Learning Techniques for Intrusion Detection System: A Review,» *International Journal of Computer Applications*, vol. 119, nº 3, p. 9, junio 2015.
- [25] B. Lhotsky, *Instant OSSEC Host-based Intrusion Detection System*, Birmingham: Packt, 2013.
- [26] K. Bittner y I. Spence, *Use case modeling*, Addison-Wesley Professional., 2003.
- [27] L. M. Á. e. a. Sabucedo, «Providing standard-oriented data models and interfaces to eGovernment services: A semantic-driven approach,» *Computer Standards & Interfaces*, vol. 31, nº 5, pp. 1014-1027, 2009.
- [28] Inflectra, «Use Cases & Scenarios: What They Are & More,» 14 septiembre 2023. [En línea]. Disponible: <https://www.inflectra.com/Ideas/Topic/Use-Cases.aspx>. [Último acceso: 16 noviembre 2023].
- [29] NATO, «Federated Mission Networking,» 29 enero 2015. [En línea]. Disponible: <https://dnbl.ncia.nato.int/FMNPUBLIC/SitePages/Home.aspx>.