Universitat Oberta de Catalunya

uoc.edu

Orquestación y respuesta ante incidentes de ciberseguridad

Sergio Sánchez Palma
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)
M1.749 - TFM-Seguridad empresarial

Manuel Jesús Mendoza Flores
Cristina Romero Tris

28/12/2021

Agradecimientos:

Se lo agradezco especialmente a mi pareja Anna por apoyarme durante el transcurso del proyecto y a mi hijo Lluc por las horas juego que le he robado y ahora recuperaremos.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Orquestación y respuesta ante incidentes de ciberseguridad*
Nombre del autor:	*Sergio Sánchez Palma*
Nombre del consultor/a:	*Manuel Jesús Mendoza Flores*
Nombre del PRA:	*Cristina Romero Tris*
Fecha de entrega (mm/aaaa):	12/2021
Titulación:	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)*
Área del Trabajo Final:	*M1.749 - TFM-Seguretat empresarial*
Idioma del trabajo:	*Español*
Palabras clave	*Orquestación, SOAR, Playbooks*

Resumen del Trabajo

Las ciberamenazas están aumento cada año y es habitual que organizaciones y particulares suframos sus consecuencias. El impacto puede ser de diversa índole, afectando a servicios básicos de la población o vidas humanas en el peor escenario.

Existen muchas tecnologías que tienen como objetivo mejorar la postura de seguridad de las organizaciones mitigando o erradicando el riesgo que estas suponen. La falta de experiencia, procedimientos y equipos técnicos limitados son un cuello de botella para su tratamiento.

En los últimos años ha aparecido una nueva tecnología denominada SOAR, que pretende automatizar aquellas acciones, habitualmente realizadas por los equipos SOC, reduciendo los tiempos de respuesta ante incidentes.

El objetivo del proyecto es generar una propuesta de valor que nos permita determinar si las herramientas SOAR son una solución.

Para ello se ha realizado un trabajo de investigación que determina los diferentes tipos de amenazas registradas y las que suponen un mayor riesgo. Con el objetivo de automatizar su respuesta. Adicionalmente se ha realizado el diseño de unos flujos de prevención y remediación que han sido probados en un entorno de laboratorio.

Los resultados obtenidos han sido satisfactorios en lo que refiere al uso de la tecnología mediante la ejecución de los casos de uso. En referencia al estudio realizado, la criticidad de los datos, la falta de un modelo de datos parar registrar incidentes que permita la analítica y solo trabajar con información agregada. No

han ayudado a establecer un criterio que ayude a priorizar el tratamiento de las diferentes amenazas.

Abstract

Cyber threats are increasing every year and it is common for organizations and individuals to experience their consequences. The impact can be of different types, affecting basic population services or human lives in the worst case.

There are many technologies that aim to improve the security posture of organizations by mitigating or eradicating the risk from threats. Lack of experience, limited technical team and lack of procedures are a delay their treatment.

In the last years, a new technology called SOAR has appeared, which aims to automate those actions, usually performed by SOC teams, reducing incident response times.

The objective of the project is to generate a value proposition that will allow us to determine whether SOAR tools are a solution.

To this purpose, an investigation work has been performed to determine the different types of threats registered and which ones represent a higher risk. With the objective of automating their response. Additionally, prevention and remediation flows have been designed and tested in a laboratory environment.

The results obtained have been satisfactory in terms of the use of technology through the implementation of use cases. In relation to the study performed, the critical nature of the data, the absence of a data model to record incidents that would allow analytics and only work with aggregated information, have not helped to determine a criteria that would help to prioritize the management of the different threats. These did not help to establish a criteria to help to prioritize the management of the different threats.

Índice

Lista de figuras

Lista de tablas

1. Introducción

1.1. Contexto y justificación del trabajo

Actualmente existe un gran número de ciberamenzas potenciales, que en muchas ocasiones se materializan poniendo en jaque a organizaciones y usuarios. El listado de consecuencias de la culminación de estas amenazas es variado y a modo de ejemplo podríamos nombrar el robo de información sensible, fraude o indisponibilidad.

Somos objeto de este tipo de amenazas o ciberataques, cualquier persona conectada directa o indirectamente a las diferentes soluciones tecnológicas que nos rodean hoy en día. Ya sea mediante el uso de nuestros dispositivos móviles, computadores o dispositivos IoT como asistentes de voz, cámaras de seguridad o imeters que monitorizan o telecontrolan servicios básicos, como por ejemplo el agua o la electricidad que llega a nuestros hogares. También se han de considerar como objetivo de estas amenazas, aquellos servicios cloud donde almacenamos de forma consciente y directa información o bien son diferentes entidades y organizaciones las que archivan gran parte de nuestra información personal como dirección, cuentas bancarias, fotos, informes médicos, nominas…

De la misma forma los diferentes tipos de organizaciones, tanto del sector público como privado, se enfrenan a estos mismos retos e incluso mayores, pues la información es como norma general el activo más valioso y por este motivo son objeto de deseo de los atacantes. Además, existe el hándicap de que estas, han de proteger toda información que custodian desde estos tres puntos de vista confidencialidad, integridad y disponibilidad.

Adicionalmente, la necesidad de tener presencia online y la venta de servicios por este medio hace que la superficie de ataque sea más amplia aumentando las posibilidades de que los ataques se materialicen.

Afortunadamente, en los últimos 10 años se han sumado gran cantidad de soluciones a las ya existentes para dar respuesta a los diferentes tipos de amenazas que han ido apareciendo. No es un secreto que las diferentes empresas han aumentado sus inversiones en materia de ciberseguridad empujados por diferentes legislaciones como podría ser la GDPR y sanciones más severas ante el incumplimiento de ellas.

No obstante, uno de los problemas principales radica en el uso de una gran diversidad de nuevas tecnologías, por usuarios no expertos o sin formación suficiente para gestionar toda la tecnología que tienen a su alcance de forma adecuada y ágil.

Como solución a los problemas derivados del gran volumen de nuevas tecnologías que aumentan funcionalidades de forma constante, la falta de experiencia o recursos humanos para gestionarla adecuadamente y el alto

número de usuarios no formados en matera de ciberseguridad; han potenciado la necesidad de contar con procedimientos y automatismos para la gestión y tratamiento de las amenazas. Por ello, en los últimos años han aparecido diferentes soluciones tecnológicas catalogadas como herramientas SOAR (Security Orchestration, Automation and Response). La tecnología SOAR sin pretender ser una tecnología SIEM permite gestionar alertas de diferentes fuentes, estandarizando procesos mediante el uso de “playbooks” o casos de uso, pudiendo automatizar la respuesta de estas alertas.

Desde un punto de vista académico, el objetivo general del proyecto será el de crear una propuesta de valor que permita determinar si se puede mejorar la postura de seguridad de las organizaciones mediante el uso de herramientas SOAR.

Para ello, ha realizado un trabajo de investigación previo para analizar los siguientes puntos:

- Identificar que amenazas conocidas y registradas son las que se suceden.
- Evaluar el impacto de dichas amenazas.
- Cuantificar el impacto real de estas amenazas.

El resultado de la investigación derivará en un apartado práctico donde se ha realizado una prueba de concepto (POC) con una herramienta SOAR y un laboratorio con diferentes tecnologías. La prueba de concepto consiste en la realización de diferentes casos de uso que permitirán mejorar el tratamiento de una amenaza frente un tratamiento de manual. La experiencia de la prueba de concepto deberá traducirse en:

- La creación de una serie de casos de uso que permita abordar diferentes tipos de amenazas.

1.2. Objetivos del trabajo

El objetivo general del trabajo es “generar una propuesta de valor que permita mejorar la postura de seguridad de las organizaciones mediante el uso de herramientas SOAR”.

Este objetivo general se apoyará en el siguiente listado de objetivos específicos acotados y distribuidos en las diferentes fases del proyecto definidas en el enfoque y método seguido de trabajo.

Los objetivos específicos se describen a continuación:

- Objetivo 1: Estudio de los diferentes tipos de ciberamenzas potenciales que sufren las diferentes organizaciones y derivan en incidente.
- Objetivo 2: Análisis y definición de criterios que permita determinar estadísticamente que amenazas son más relevantes.

- Objetivo 3: Diseño y propuesta de remediación de amenazas potenciales mediante el uso de herramientas SOAR.
- Objetivo 4: Prueba de concepto en un entorno de laboratorio.

A continuación, se facilita una breve descripción de cómo se abordará cada uno de los diferentes objetivos específicos en función de las fases definidas en el apartado planificación del trabajo:

Fase 2: Investigación

Objetivo 1: Para realizar el estudio de los diferentes tipos de ciberamenzas que suceden en la actualidad, se tratará de establecer contacto con diferentes tipos de organizaciones preferiblemente públicas o sin ánimo de lucro que manejen este tipo de información. En paralelo, se realizará una búsqueda intensiva en Internet de publicaciones que puedan ser relevantes para el proyecto.

Objetivo 2. En base a la información obtenida, se procesará y evaluará con el fin de poder obtener un criterio que permita hacer foco en los tipos de amenazas más relevantes que puedan ser tratadas mediante el uso de herramientas SOAR.

Fase 3 Diseño y POC

Objetivo 3: Se realizará una selección de amenazas en base a la información obtenida y se creará un caso de uso estándar que permita abordar el problema. Dependiendo del alcance del caso de uso, se plantea la posibilidad de crear una colección de casos de uso.

Objetivo 4: Se realizará una selección de herramientas que permitan emular el comportamiento o trazas de una amenaza para que esta pueda ser tratada con la utilización de una herramienta SOAR.

Al tratarse de un proyecto académico acotado en tiempo no es fundamental que los objetivos se cumplan de forma efectiva. Existe diversos factores que podrían afectar a la calidad de los resultados de estos. Algunos de ellos se mencionan en el aparatado análisis de riesgos.

Para evaluar si se han cumplido los objetivos se calificarán con una escala del 1 al 5 cada uno de ellos de forma independiente según la siguiente tabla definida.

Puntuación	Resultado
1	Muy por debajo de lo esperado
2	Por debajo de lo esperado
3	Resultado esperado
4	Por encima de lo esperado
5	Muy por encima de lo esperado

Tabla 1 - Métrica evaluación objetivos

1.3. Enfoque y método seguido

Para la ejecución del proyecto se utilizará una metodología de trabajo organizada por fases donde se han tratado una serie de entregas obligatorias como hitos. Cada hito ha marcado el final de una fase y el inicio de la siguiente.

La planificación inicial de tareas se presenta en el siguiente apartado, planificación del trabajo, ha contemplado que podrían darse ligeras alteraciones en los tiempos y tareas. Uno de los motivos es que parte del estudio de amenazas dependería de la información aportada por terceras partes y en función de la respuesta e interés de los datos obtenidos podría justificarse una modificación en la planificación inicialmente planteada. De la misma forma las tareas de la fase de diseño y prueba de concepto se contempla que podrían verse modificadas en tiempo o incrementadas por la dependencia sobre el estudio e investigación realizados en la fase de investigación. En ningún caso se ha contemplado la opción de modificar las fechas de los hitos.

El proyecto constará de dos secciones diferenciadas en el marco global del proyecto que serán clave para alcanzar el objetivo general del proyecto.

Investigación:

Se ha asociado la investigación, a la fase 2 de la planificación. Se han abierto dos líneas de investigación en paralelo. En la primera línea se tratará de establecer contacto con diferentes organizamos y entidades con el fin de obtener información de ciberamenzas con un alto nivel de calidad y veracidad. En paralelo se abre una segunda línea de investigación tratando de obtener información de carácter público que permita la continuidad del proyecto en caso de que la primera línea de actuación fracase, debido a la falta de proactividad por parte de terceros o bien a la negativa de facilitar la información solicitada debido a la criticidad de esta.

Esta fase incluirá también la creación de un criterio que permita realizar una selección de las amenazas más relevantes donde un sistema SOAR pueda mejorar el estado de protección de las diferentes organizaciones.

Diseño y POC**:**

A partir de los resultados obtenidos y del estudio de las amenazas realizas en la fase anterior, se establecerá un marco genérico pendiente de definir donde se tendrán en cuenta diferentes soluciones de seguridad como: Firewalls, IDS/IPS, SIEM, Sandbox, MISP, Antivirus, NAC… En base a este marco se realizará un diseño de casos de uso cuyo número se decidirá en base a la complejidad de estos o la estrategia definida para abordar el problema. La finalidad de los casos de uso será la de tratar la amenaza ya sea mediante acciones de mitigación, remediación y/o erradicación. O bien realizando su tratamiento a posteriori, facilitando las

tareas de averiguar qué ha sucedido, cual ha sido el alcance real o dando respuesta a otras cuestiones.

Una vez realizado el diseño o diseños se efectuará una prueba de concepto que sirva de muestra de cómo al menos uno de los diseños, puede ser implementado en una herramienta de orquestación.

En lo que refiere a la ejecución de la POC, y tras la selección de herramientas a implementar, un punto a tener en cuenta es su despliegue. Dicho despliegue no se entiende como una parte importante en el resultado final del proyecto, sino la interconexión y orquestación de acciones. Por este motivo no se documentará ningún proceso de instalación de las herramientas utilizadas.

Redacción memoria:

Será en la fase 4 donde se sintetizarán los resultados y donde se realizará la propuesta de valor en base a la investigación realizada y la experiencia adquirida durante la parte práctica del proyecto.

El principal motivo por el cual se ha elegido esta estrategia de trabajo por fases es la necesidad de realizar entregas parciales durante el transcurso del proyecto, la corta duración temporal del mismo y que el trabajo se realiza de forma independiente sin contar con un equipo de dos o más personas ni dependencias de los resultados de otros proyectos en curso.

1.4. Planificación del trabajo

A continuación, se listan los recursos necesarios para realizar el proyecto y la planificación asociada al mismo. Las rectificaciones y replanificaciones realizadas no son destacables en tiempo de dedicación y se encuentran en los ficheros anexos al proyecto, pero no en la siguiente planificación inicial.

Listado de recursos necesarios para la ejecución del proyecto:

- Información estadística de tipos de amenazas detectadas y categorizadas.
- Herramienta de gestión de proyectos
- Suite ofimática
- Herramienta creación diagramas
- Herramienta de grabación de videos.
- Solución de Backups
- Hardware con capacidades de virtualización
- Software de virtualización
- Suite de herramientas de ciberseguridad
- Internet

Planificación del proyecto:

Título	Fecha de inicio	Fecha de vencimiento	Duración
TFM (programación inicial)	**15/09/2021**	**14/01/2022**	
1. Plan de trabajo			
Redacción entregable 1	15/09/2021	28/09/2021	14 días
Preparación entorno de trabajo	19/09/2021	20/09/2021	2 días
Planificación	26/09/2021	27/09/2021	2 días
Definir Tareas	26/09/2021	27/09/2021	1 día
Calcular tiempos	27/09/2021	27/09/2021	1 hora
Identificar Riesgos	27/09/2021	27/09/2021	1 hora
Definir costes	27/09/2021	27/09/2021	1 hora
Definir metodología	24/09/2021	24/09/2021	1 día
Definición de objetivos	23/09/2021	23/09/2021	1 día
Problema a resolver	15/09/2021	21/09/2021	7 días
Entrega 1		28/09/2021	
Estado del arte	21/09/2021	21/09/2021	1 día
Lectura Redacción de trabajos académicos	15/09/2021	15/09/2021	1 día
Recursos necesarios	25/09/2021	25/09/2021	1 día
2. Investigación			
Determinar Criterio de selección	25/10/2021	26/10/2021	2 días
Estudio de los datos	13/10/2021	24/10/2021	12 días
Obtención de Información	27/09/2021	18/10/2021	22 días
Obtención datos de organizaciones	27/09/2021	18/10/2021	22 días
Obtención información de fuentes públicas en Internet	27/09/2021	12/10/2021	16 días
Redacción entregable 2	27/09/2021	26/10/2021	30 días
Entrega 2		26/10/2021	
3. Diseño y POC			
POC	05/11/2021	23/11/2021	19 días
Preparar entorno	05/11/2021	09/11/2021	5 días
Implementar playbooks	10/11/2021	19/11/2021	10 días
Pruebas y Testeo de los playbooks	20/11/2021	23/11/2021	4 días
Diseño de casos de uso	27/10/2021	04/11/2021	9 días
Redacción entregable 3	27/10/2021	23/11/2021	28 días
Entrega 3		23/11/2021	
4. Memoria final			
Crear propuesta de valor	24/11/2021	30/11/2021	7 días
Redacción de la memoria	24/11/2021	28/12/2021	35 días
Entrega 4		28/12/2021	
5. Presentación en vídeo			
Creación del video de presentación de la memoria	29/12/2021	04/01/2022	7 días

Entrega 5		04/01/2022	
6. Defensa del TFM			
Defensa		14/01/2022	
Resolución de cuestiones	10/01/2022	14/01/2022	5 días
Total: 35 tareas			

Tabla 2 - Planificación del proyecto

El tiempo de dedicación en número de horas o días, puede variar en función de tarea a completar. El número de días u horas marcan el límite de tiempo objetivo para finalizar las tareas en el periodo estipulado.

A continuación, se muestra la planificación temporal por fases e hitos en un diagrama de Gantt.

Planificación Hitos (Gantt)

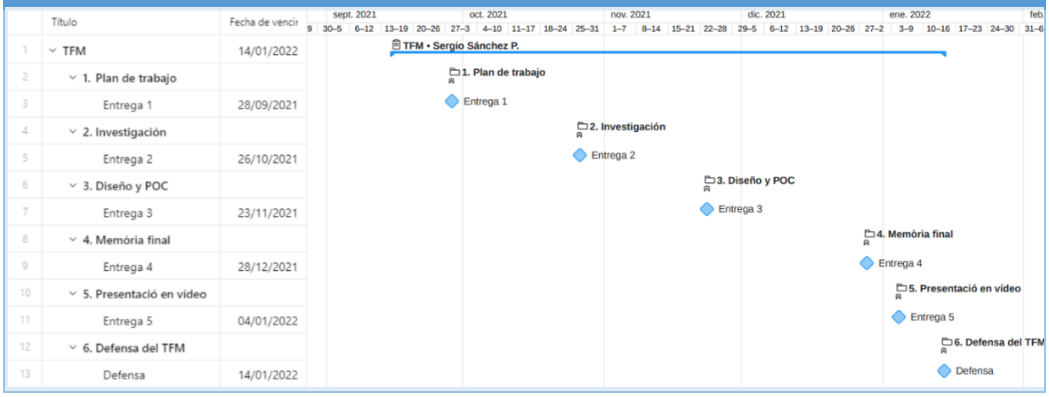


Tabla 3 - Planificación hitos Gantt

Planificación por fases (Gantt)

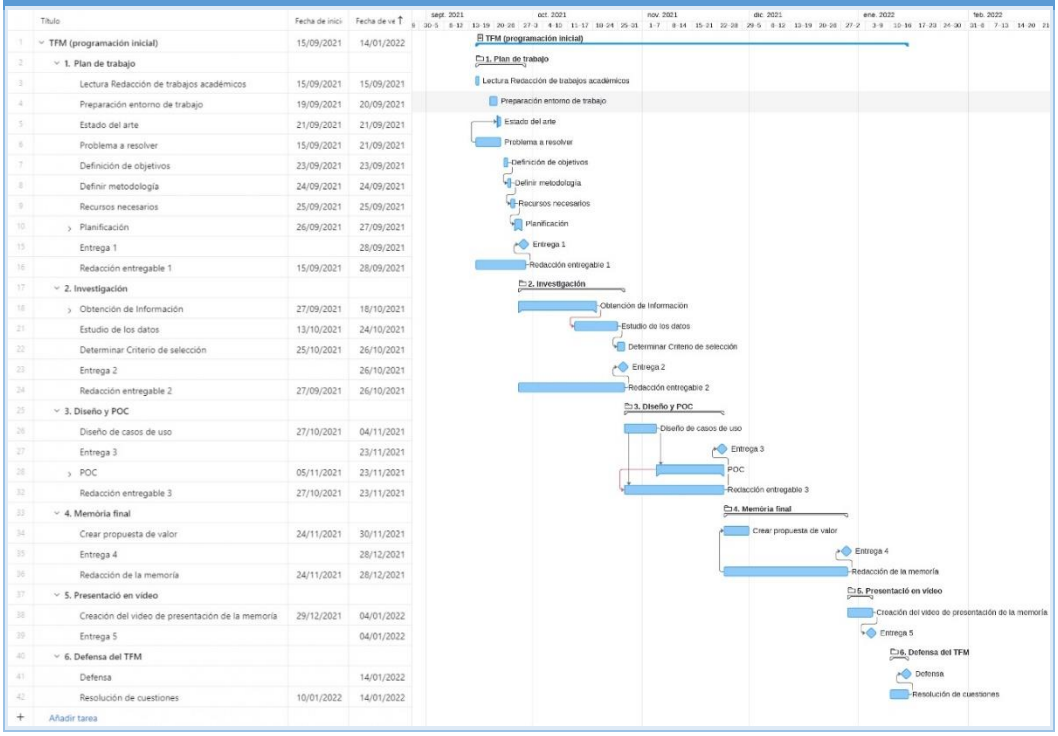


Tabla 4 - Planificación por fases Gantt

En los anexos al proyecto se incorpora la planificación inicial del proyecto y la planificación final ejecutada con las replanificaciones realizadas y reportadas durante la ejecución de este.

1.5. Presupuesto del proyecto

Para la ejecución del proyecto se estipulo la máxima de minimizar los gastos tanto en software como en hardware todo lo que fuera posible evitando afectar a la calidad de los resultados de forma notable.

En lo que refiere al software se han utilizado licencias de carácter gratuito para estudiantes o versiones de evaluación. Aunque no estaba previsto ningún tipo de gasto en este aspecto se ha optado adquirir una licencia para obtener información de credenciales filtradas con un coste simbólico.

En lo que refiere al hardware, uno de los objetivos es realizar una prueba de concepto. Se contempló que la prueba de concepto podía tener una alta probabilidad de que se necesitaran recursos hardware muy elevados no siendo posible la realización de esta en un equipo de hogar estándar.

Excluimos del presupuesto aquellos elementos con los que ya contaba antes del inicio del proyecto como es PC personal y periféricos, conexión a Internet, necesarios para la realización del proyecto. El motivo de la exclusión es que si se realizará el despliegue en un entorno empresarial la matriz de costes y gastos asociados no sería extrapolable. Sí solo nos centramos en los costes de implementación y uso de los casos de uso, el coste asociado en un entorno empresarial dependerá del tipo de tecnologías utilizadas, acuerdos comerciales, numero de analistas en el equipo del SOC. Por lo tanto, los costes estimados presentados solo hacen referencia al proyecto.

Se ha previsto una partida máxima de 373,89€ para alquilar hardware en formato IaaS durante 3 meses en el caso de que fuera necesario y siempre que se diera el peor de los escenarios posibles. Se descarta el uso de sistemas cloud como Azure, AWS o similares con el objetivo de gestionar mejor el gasto.

Se ha seleccionado un servidor que podría satisfacer de forma adecuada las necesidades de disco duro, RAM y CPU que podrían surgir para la realización de la parte práctica del proyecto. Se ha de mencionar que la estimación ha sido previa a la ejecución de la POC y a continuación se presentará tanto la estimación previa como los costes finales de hardware y licencias.

Estimación de costes inicial:

Se estimó un coste de uso de un servidor con capacidades de virtualización durante un periodo de tres meses de 254,10€ con IVA +

119,79€ con IVA por la puesta en marcha, el cual se trataría de negociar con el proveedor para que lo deje a coste 0€.

Las características del servidor físico que se utilizaría para crear un entorno de virtualización son las siguientes.

Proveedor	OVH
Descripción	Servidor dedicado Rise-3 Este servidor, diseñado para satisfacer requerimientos de recursos muy exigentes, ofrece un buen equilibrio entre la potencia de su procesador Intel y la memoria DDR4 de 64 GB.

Procesador:	Intel® Xeon® E5-1650v4
Coste	69,99 € + IVA/mes Instalación: 99,99 € + IVA
Ubicación	Francia (Gravelines - GRA)
Tiempo de entrega	120s
Procesador	Intel Xeon E5-1650v4 - 6c/ 12 t - 3.6GHz / 4GHz
Memoria	64 GB DDR4 ECC 2133 MHz
Almacenamiento	2 x 2 TB HDD SATA Soft RAID
Ancho de banda público:	500Mb/s, ilimitado

Tabla 5 - Característica servidor de contingencia

Costes finales del proyecto:

Ha sido necesario utilizar parte de los recursos hardware adicionales previstos en el análisis de riesgos y a continuación se presenta el desglose de gastos realizados para la ejecución del proyecto.

Recurso	Uso	Coste final
Hardware		
8c-3,6Ghz/64GB/1TB	Infraestructura de virtualización	169,37€
Software		
Have I Been Pwned	Obtención información credenciales filtradas	3,28€

Tabla 6 - Costes del proyecto

Coste Total: 172.65€ con IVA.

1.6. Análisis de riesgos

Durante la fase inicial del proyecto se ha realizado un ejercicio donde se trata de identificar y enumerar posible riesgos o situaciones que podrían afectar desfavorablemente a la realización del trabajo.

Para determinar de forma cualitativa el riesgo derivado de cada uno de los supuestos, aplicaremos la siguiente metodología para calcular el riesgo. Se aplica una matriz de riesgo como resultado de cruzar la probabilidad estimada de que se produzca un riesgo por el impacto de este.

Como resultado se presentan una serie de planes de mitigación que garanticen en éxito del proyecto.

Tabla probabilidad:

Cualitativo	Descripción
Baja	Muy poco probable de que suceda
Media	Podría suceder
Alta	Muy probable de que suceda

Tabla 7 - Cálculo de probabilidad

Tabla cálculo de impacto:

Cualitativo	Descripción
Bajo	El daño en caso de que suceda no tiene consecuencias importantes en el TFM
Medio	El daño en caso de que suceda tendría consecuencias destacables en el TFM
Alto	El daño en caso de que suceda afectaría a la finalización del TFM

Tabla 8 - Cálculo de impacto

Para calcular el riesgo se aplicará la siguiente formula multiplicando los factores de probabilidad e impacto.

Tabla cálculo del riesgo:

		Impacto		
		Bajo	*Medio*	*Alto*
Probabilidad	*Baja*	Muy bajo	Bajo	Medio
	Media	Bajo	Medio	Alto
	Alta	Medio	Alto	Muy alto

Tabla 9 - Cálculo del riesgo

Listado de riesgos identificados y planes de mitigación:

Riesgos identificados	Probabi-lidad	Impac-to	Riesgo	Mitigación
Retardos en las entregas	Baja	Alto	Medio	Uso de herramienta de gestión de proyectos con notificaciones sobre el inicio y final de las diferentes tareas.
Retardos en la definición de los casos de uso	Baja	Alto	Medio	Ante un posible retardo y para no afectar a los objetivos se revisaría si el alcance inicial es demasiado ambicioso y se reduciría.

No obtención de información fidedigna	Media	Medio	Medio	Como alternativa se obtendrá la información publicada de mayor calidad que se pueda encontrar en la red y se realizará el estudio en base a dicha información.
Baja calidad de los entregables	Baja	Medio	Bajo	Para evitarlo, se trabajará con la plantilla de la memoria final del proyecto en las entregas asociadas a los diferentes hitos del proyecto.
Mala planificación	Baja	Alto	Medio	Ante una mala planificación, se replanificarán y / o modificarán las tareas sin afectar a objetivos e hitos.
Falta de información clave	Media	Medio	Medio	Se reevaluará el alcance y se buscaran alternativas que permitan el avance del proyecto.
Problemas de conectividad	Baja	Alto	Medio	Se utilizaría un plan de datos móvil como alternativa.
Perdida de información total o parcial	Baja	Alto	Medio	Se realizarán backups periódicos en un disco duro externo no conectado permanentemente al PC. Se hará uso de la cuenta gratuita de office365 para estudiantes y se trabajará desde carpetas sincronizadas con OneDrive.
Falta de medios técnicos suficientes para ejecutar la POC	Alta	Alto	Muy Alto	Se ha reservado una partida económica para adquirir infraestructura como servicio en caso de que fuera necesario.
Dificultad en despliegue y uso de herramientas	Alta	Medio	Alto	Se hará uso de herramientas ya preconfiguradas para reducir los tiempos e instalación y configuración de estas.
Necesidad de licencias de pago para realizar POC	Baja	Bajo	Baja	Se hará uso en la medida de lo posible uso de versiones gratuitas para estudiantes, software opensource o en su defecto se solicitarían versiones de evaluación.

Tabla 10 - Riesgos identificados y mitigación

1.7. Estado del arte

Este apartado realizado al inicio del proyecto nos introducirá y ayudará a establecer un marco de trabajo ampliando el contexto y justificación del trabajo. Ha sido necesario realizar un estudio más amplio durante el transcurso del proyecto. Tratando de establecer un contacto directo con entidades que se abstraigan lo máximo posible del ámbito comercial.

Para conocer el estado actual y los retos de ciberseguridad que hay en la actualidad, se ha realizado un breve análisis previo a la investigación utilizando como fuentes de referencia documentos publicados por INCIBE, CCN-CERT, Palo Alto Networks, Splunk cuyas referencias se encuentran en el apartado de bibliografía.

Podemos resumir que en la actualidad las necesidades de conectividad van en aumento, bajo el contexto de pandemia por la covid-19 las necesidades de conectividad remota han crecido, acelerando el proceso de transformación digital de muchas compañías. Es en este contexto encontramos que muchos empleados fuera del ámbito IT han tenido que hacer uso de conexiones remotas a sus compañías por primera vez para poder trabajar. En ocasiones con equipos no corporativos e incluso de uso compartido en los hogares.

Las organizaciones han priorizado las inversiones en tecnologías para facilitar las opciones de conectividad. Es en estas inversiones donde se apuesta por el uso de tecnologías Cloud. Ya sea por la inmediatez en los despliegues respecto a sistemas on-premise o bien por las bajas necesidades de mantenimiento de la infraestructura. Uno de los riesgos derivados de este tipo de tecnologías es la pérdida del gobierno del dato en ocasiones.

Por lo tanto, tenemos varios aspectos importantes a considerar; mayor necesidad de conectividad, equipos con nivel de protección bajos, usuarios inexpertos materia de seguridad o no suficientemente concienciados sobre los riesgos tecnológicos y gran cantidad de tecnologías, en ocasiones nuevas.

En paralelo, el número de ataques conocidos va en aumento, conforme aumentan las opciones tecnológicas y la publicación de accesos a herramientas en la red hace crecer el nivel de exposición y superficie de ataque. Además, siguen surgiendo nuevas técnicas de ataque y se mejoran algunas de las existentes.

"…el uso de la tecnología sigue su tendencia alcista, también se incrementan los problemas de ciberseguridad."[1]

Para entender a que se deben estos ataques es importante saber que actores se encuentran detrás de ellos, cada uno con diferentes motivaciones. Estados, ciberdelincuentes, ciberterroristas, hacktivistas y usuarios internos son los principales actores.

En mayor o menor medida muchas organizaciones públicas o privadas cuentan con políticas, sistemas y equipos de personas para abordar diferentes tipos de amenazas. En especial, las empresas con mayor inversión en tecnologías cuentan con equipos humanos especializados que monitorizan, gestionan las diferentes amenazas y participan en la toma de decisiones para que el entorno empresarial desde el punto de vista de las tecnologías de la información y comunicación sea más seguro. No obstante, a mayor volumen de tecnología e información, crece la dificultad en la tarea de analíticas de ciberseguridad y se dificulta la priorización y tratamiento de las amenazas.

[1] Informe: Cyber amenazas y tendencias ed.2020, pg.6, Centro Criptológico Nacional

Existen dos hándicaps añadidos. La globalización hace que los diferentes ataques puedan producirse en cualquier momento y la capacidad de resolución de los equipos es limitada. A modo de ejemplo, si un equipo de seguridad trabaja en un incidente como un ransomware es probable que no tenga la capacidad para poder detectar e identificar otros tipos de amenazas que puedan producirse en paralelo. De la misma forma pueden producirse episodios donde la gestión de amenazas suponga un cuello de botella y afecte al funcionamiento habitual de las empresas.

Como solución a este tipo de problemas surgen herramientas denominadas SOAR. Las cuales tiene como objetivo automatizar gran parte de los procesos de detección, análisis y resolución de amenazas, ya sea de forma total o parcial.

2. Investigación

En la planificación del trabajo, se definió que se abrían dos líneas de investigación en paralelo.

En la primera línea se trataría de establecer contacto con diferentes organizamos y entidades con el fin de obtener información sobre ciberamenzas con un alto nivel de calidad y veracidad. Los resultados de dichas líneas de investigación los podemos ver en el apartado obtención datos organizaciones del presente documento.

En la segunda línea de investigación se trataría de obtener información de carácter público no asociada a organismos públicos que permita la continuidad del proyecto, en caso de que la primera línea de actuación fracasase. Dicho fracaso podría estar condicionado a una posible falta de proactividad por parte de terceros o bien a la negativa de facilitar la información solicitada debido a la criticidad de esta. Los resultados de dichas líneas de investigación los podemos ver en el apartado obtención información fuentes públicas.

2.1. Obtención de información

2.1.1. Obtención datos organizaciones

La obtención de datos de las organizaciones es la primera línea de actuación donde se ha tratado de establecer contacto con diferentes organizamos y entidades de carácter público con el fin de obtener información veraz sobre los diferentes tipos de amenazas que sufren las organizaciones ya sean publica o privadas.

Las principales entidades con las que se ha tratado de establecer contacto para conseguir información de carácter restringido o no publicada han sido las siguientes:

- Centro Criptológico Nacional, (CCN-CERT)
- Instituto Nacional de Ciberseguridad (INCIBE)
- Oficina de Seguridad del Internauta (OSI)

El objetivo de establecer estos contactos de forma efectiva no ha sido cumplido y no se han materializado de la forma esperada. Ya sea por ausencia de respuesta o por derivación a fuentes de información públicas y ya identificadas previamente. Se esperaba de este contacto obtener la suficiente información en crudo como para poder determinar de forma independiente cuales son los problemas reales de las organizaciones en materia de ciberseguridad.

Las principales fuentes objeto de recolección de información publicada han sido las siguientes:

- Observatorio Nacional de Tecnología y Sociedad
- Observatorio Español de Delitos Informáticos (OEDI)
- Ministerio del Interior (MIR)
- Centro Criptológico Nacional Computer Emergency Response Team (CCN–CERT)
- Dirección General de Coordinación y Estudios

A continuación, se describirán por organización, quienes son y la información más actualizada que dichas organizaciones aportan a la sociedad en materia de ciberseguridad. Para ello se han analizado los puntos más relevantes de sus diferentes publicaciones con el objetivo de obtener los principales riesgos y problemas a resolver con el uso de herramientas SOAR.

Observatorio Nacional de Tecnología y Sociedad

¿Quiénes son?

El ONTSI es el Observatorio Nacional de Tecnología y Sociedad, siendo su propósito el de generar conocimiento de valor para las políticas públicas (así como para la intervención empresarial y ciudadana) en torno al desarrollo tecnológico y sus distintos impactos en la economía, el empleo, los servicios públicos, los derechos, la seguridad, la calidad de vida y la igualdad entre las personas.[2]

¿Cómo nos ofrecen la información?

Cuentan con una herramienta web llamada ONTSI.data que nos permitirá elaborar nuestros propios informes con los principales indicadores de la Sociedad de la Información, del sector de las Tecnologías de la Información y las Telecomunicaciones para España, países de la Unión Europea y miembros de la OCDE.

[2] Web: Observatorio Nacional de Tecnología y Sociedad, (28 de 12 de 2021) https://www.ontsi.es/es/Que-hacemos

Ilustración 1 - Portal web consulta de datos ontsi.data[3]

Tras revisar la información aportada solo nos permite obtener información del año 2019 sumariada y sin detalle suficiente como para poder conocer los sistemas de clasificación utilizados. Por lo tanto, se descarta el uso de este origen de datos.

Observatorio Español de Delitos Informáticos (OEDI)

¿Quiénes son?

OEDI nace a partir de la necesidad de dar a conocer el problema del aumento de los delitos informáticos en España, buscando informar a la sociedad sobre la legislación vigente en materia de ciberdelitos y fomentando la realización de denuncias formales ante los organismos competentes.[4]

¿Cómo nos ofrecen la información?

En primer lugar, es importante tener una breve definición de que es un delito informático según la legislación española. “Delito informático, delito cibernético o ciberdelito es toda aquella acción antijurídica que se realiza en el entorno digital, espacio digital o de Internet”[5].

A partir de esta descripción nos encontramos con una clasificación basada en diferentes tipos de Ciberdelitos según la legislación española

Las siguientes tablas se han generado con la información obtenida de la web de OEDI e indican en función de los artículos penales como se clasifican los diferentes tipos de delitos.

[3] Link: https://servicesqap.red.es/single/?appid=c39c3c09-4e12-4485-b662-ee2673c46ec2&sheet=b7571d1f-4979-484d-aa73-02ee06fe749f

[4] Web: Observatorio español de delitos informáticos, (28 de 12 de 2021) https://oedi.es/

[5] Web: Wikipedia, (28 de 12 de 2021) https://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

Acceso e interceptación ilícita	
Código Penal español	Art. 197 a 201. Descubrimiento y revelación de secretos Art. 278 a 286. Delitos relativos al mercado y los consumidores (espionaje industrial)
Tipo de hecho	Descubrimiento/revelación de secretos Acceso ilegal informático Otros relativos al mercado/consumidores
Variables y medios empleados	Internet/informática, telefonía/comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Tabla 11 - Acceso e interceptación ilícita

Interferencia en los datos y en el sistema	
Código Penal español	Arts. 263 a 267 y 625.1. Daños y daños informáticos
Tipo de hecho	Daños Ataques informáticos
Variables y medios empleados	Internet/informática, telefonía/comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Tabla 12 - Interferencia en los datos y en el sistema

Falsificación informática	
Código Penal español	Arts. 388-389, 399 bis, 400 y 401
Tipo de hecho	Falsificación de moneda, sellos y efectos timbrados Fabricación tenencia de útiles para falsificar Usurpación del estado civil
Variables y medios empleados	Internet/informática, telefonía/comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Tabla 13 - Falsificación informática

Fraude Informático	
Código Penal español	Arts. 248 a 251 y 623.4
Tipo de hecho	Estafa bancaria: Estafas con tarjetas de crédito, débito y cheques de viaje Otras estafas
Variables y medios empleados	Internet/informática, telefonía/comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Tabla 14 - Fraude Informático

Delitos sexuales	
Código Penal español	Arts. 181, 183.1, 183.bis,184, 185, 186 y 189
Tipo de hecho	Exhibicionismo Provocación sexual Acoso sexual Abuso sexual Corrupción de menores/incapacitados Pornografía de menores Delito de contacto mediante tecnología con menor de 13 años con fines sexuales

Variables y medios empleados	Internet/informática, telefonía/comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Tabla 15 - Delitos sexuales

Contra la propiedad industrial intelectual	
Código Penal español	Arts. 270 a 277 y 623.5 (Contra la propiedad intelectual y contra la propiedad industrial)
Tipo de hecho	Delitos contra la propiedad industrial Delitos contra la propiedad intelectual
Variables y medios empleados	Internet/informática, telefonía/comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Tabla 16 - Contra la propiedad industrial intelectual

Contra el honor	
Código Penal español	Arts. 205 a 210 y 620.2
Tipo de hecho	Calumnias Injurias
Variables y medios empleados	Internet/informática, telefonía/comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Tabla 17 - Contra el honor

Delitos contra la salud pública	
Código Penal español	Arts. 359 a 371
Tipo de hecho	Tráfico de drogas Otros contra la salud pública
Variables y medios empleados	Internet/informática, telefonía/comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales

Tabla 18 - Delitos contra la salud pública

Amenazas y coacciones	
Código Penal español	Arts. 169 a 172 y 620
Tipo de hecho	Amenazas Amenazas a grupo étnico cultural o religioso Coacciones
Variables y medios empleados	Internet/informática, telefonía/comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Tabla 19 - Amenazas y coacciones

La información aportada no es suficiente para determinar qué tipo de casos de uso pueden ser los más interesantes a realizar. El principal inconveniente es que hablamos de delitos y no existe una legislación lo suficientemente madura que contemple delitos específicos y bien definidos que hagan referencia a amenazas tecnológicas. Podemos afirmar que se han tratado de adecuar las amenazas tecnológicas a un sistema de delitos ya existentes en el código penal.

No obstante, esta información puede ser muy interesante para el proyecto si diseñamos un sistema de clasificación que nos permita registrar si un incidente de seguridad o brecha es delito o no.

Una de las ventajas de los sistemas SOAR son las capacidades de adaptación a las necesidades de los diferentes SOC o usuarios participes en los procesos de remediación o investigación. Es por este motivo que con independencia de si el sistema de clasificación puede ser más o menos útil nos permitirá poner a prueba las capacidades de los sistemas SOAR.

Existen diversos sistemas de clasificación ofrecidos por SANS, NIST, MITRE incluso GDPR, pero no es habitual contar con una relación directa que determine sí un incidente puede estar tipificado como delito o no, según legislación del país. Por lo tanto, se tratará de armar un sistema de clasificación en base a estos criterios.

Respecto a la información sumariada más actualizada que nos ofrece OEDI es la siguiente:

Estadísticas ciberdelitos año 2019

Ciberdelitos	Total
Fraude informático	192.375
Amenazas y coacciones	12.782
Falsificación informática	4.275
Acceso e interceptación ilícita	4.004
Contra el honor	1.422
Delitos sexuales	1.774
Interferencia en los datos y en el sistema	1.473
Contra la propiedad industrial/intelectual	197
Delitos contra la salud pública	0
Total	**218.302**

Tabla 20 - Estadística ciberdelitos España 2019

Los datos aportados en la tabla anterior hacen referencia a que han sido publicados por el Ministerio del Interior de España.

Ministerio del Interior

¿Quiénes son?

El Ministerio del Interior (MIR) de España es el Departamento de la Administración General del Estado responsable de la propuesta y ejecución de la política del Gobierno de la Nación en materia de la

seguridad ciudadana (fuerzas y cuerpos de seguridad del Estado, instituciones penitenciarias, protección civil, seguridad vial, etc.).[6]

¿Cómo nos ofrecen la información?

Nos ofrecen información mediante la publicación de diferentes estudios realizados. Hemos analizado en particular el siguiente estudio que se encuentra en la bibliografía del proyecto, Estudio sobre la cibercriminalidad en España en 2019.

Del estudio realizado de información se han seleccionado dos tipos graficas para tener una foto clara sobre como orientar los siguientes pasos del proyecto:

En primer lugar, se ha seleccionado la tabla donde se facilita el sumario con la información que cuenta el ministerio del interior según el delito. Es destacable el hecho de que no se facilita el detalle de las amenazas en ningún lugar del documento, simplemente totales.

HECHOS CONOCIDOS	2016	2017	2018	2019
ACCESO E INTERCEPTACIÓN ILÍCITA	3.243	3.150	3.384	4.004
AMENAZAS Y COACCIONES	12.036	11.812	12.800	12.782
CONTRA EL HONOR	1.546	1.561	1.448	1.422
CONTRA PROPIEDAD INDUST./INTELEC.	129	121	232	197
DELITOS SEXUALES(*)	1.231	1.392	1.581	1.774
FALSIFICACIÓN INFORMÁTICA	3.017	3.280	3.436	4.275
FRAUDE INFORMÁTICO	70.178	94.792	136.656	192.375
INTERFERENCIA DATOS Y EN SISTEMA	1.336	1.291	1.192	1.473
Total HECHOS CONOCIDOS	92.716	117.399	160.729	218.302

Ilustración 2 - Evolución de hechos conocidos por categoría delictiva [7]

Tras analizar la información se puede determinar que las fuentes públicas relacionadas con organismos gubernamentales están trabajando con el mismo tipo de información y sistema de clasificación. Se puede observar que los valores coinciden con los que nos ofrecen el Observatorio Español de Delitos Informáticos (OEDI) mostrados en la Tabla 20 - Estadística ciberdelitos España 2019.

El documento analizado contempla información que hace referencia a infraestructuras críticas a partir de la información de incidentes gestionados por el CERT de INCIBE. Debido a la criticidad de estos entornos, las estadísticas obtenidas pueden servir para determinar qué tipo de incidentes pueden tener un mayor impacto.

"las infraestructuras críticas son todos aquellos sistemas físicos o virtuales que facilitan funciones y servicios esenciales para apoyar a los

[6] Web: Wikipedia, (28 de 12 de 2021) https://es.wikipedia.org/wiki/Ministerio_del_Interior_(Espa%C3%B1a)
[7] Informe: Estudio sobre la cibercriminalidad ed.2019, pg.36, Ministerio del Interior

sistemas más básicos a nivel social, económicos, medioambiental y político."[8]

A continuación, se presentan dos tablas de información de incidentes donde en base al mismo sistema de clasificación podemos ver la afectación global reportada de las organizaciones y el subconjunto de ellas que son infraestructura critica.

Tipo de incidente	INCIDENTES GESTIONADOS				
	2015	2016	2017	2018	2019
Intrusión	16.054	14.373	19.275	8.541	6.479
Fraude	13.410	11.843	11.959	55.932	31.938
Malware	15.177	76.811	81.090	27.016	27.358
SPAM	1.275	10.279	7.957	0	0
Disponibilidad	794	495	514	100	58
Intento de intrusión	335	381	1.435	396	1.518
Robos de información	26	37	47	63	77
Contenido Abusivo				9.353	4.064
Recolección de información				5.605	84
Sistema Vulnerable				3.731	31.414
Otros	2.905	1.038	787	782	4.407

Ilustración 3 - Incidentes gestionados por el INCIBE-CERT[9]

Si analizamos los incidentes por cantidad podemos determinar que de mayor número de incidentes reportados a menor este es el TOP 3

1. Fraude
2. Sistemas vulnerables
3. Malware

Aquellos que se encuentran en el TOP 3 de incidentes reportados, nos sugiere que el tratamiento de estos incidentes de forma automatizada tendría un mayor beneficio ya que se descargaría a los diferentes equipos que componen un SOC, operadores, analistas, forenses, … de gran carga de trabajo. Cabe destacar que existen una gran cantidad de herramientas para detectar sistemas vulnerables y malware que forman parte del porfolio de la mayoría de las organizaciones. Esto podría indicar que gracias a la facilidad detección de este tipo de amenazas es normal que tengamos unos valores muy altos respecto a otros tipos de amenazas.

Es interesante añadir, a modo de ejemplo, que podríamos considerar un incidente de seguridad el uso de un pendrive con un malware que ha sido detectado y puesto en cuarentena por un antivirus al conectarlo a un PC. Ese mismo incidente de seguridad también lo podríamos contabilizar como uno, si el malware se ha ejecutado de forma satisfactoria y ha sido capaz de contactar contra un C&C, recolectar información y enviarla fuera de la organización. Por lo tanto, una mayor ratio de detección no siempre significa que sea el punto más importante donde focalizar los esfuerzos. Sería muy interesante conocer, clasificar y registrar el impacto de los

[8] Web: Lisainstitute, (28 de 12 de 2021) https://www.lisainstitute.com/blogs/blog/infraestructuras-criticas

[9] Informe: Estudio sobre la cibercriminalidad ed.2019, pg.33, Ministerio del Interior

diferentes incidentes de seguridad y si estos suponen una brecha de seguridad o no.

Si en cambio realizamos el TOP 3 en sentido inverso, es decir, de menor número de incidentes a mayor es el siguiente:

1. Disponibilidad
2. Recolección de información
3. Intento de intrusión

Spam: Queda descartado por una modificación en el sistema clasificación realizado en el informe que ha derivado en que el valor sea cero.

Estos tipos de categoría sugieren que el nivel de madurez para detectar e identificar este tipo de incidentes es más bajo que los que se encuentran en el TOP3 superior. Es por este motivo que se han contemplado dos de estas categorías (Recolección de información e intento de intrusión) en la realización de los casos de uso. El objetivo es dar una solución o mitigar de forma temprana los riesgos derivados de estas amenazas que pueden pasar desapercibidas.

Finalmente presentamos los datos que nos reportan relacionado con infraestructuras criticas las cuales podría tener un impacto sobre la vida de las personas o recursos en caso de sufrir un incidente.

Tipo de incidente	INCIDENTES GESTIONADOS				
	2015	2016	2017	2018	2019
Intrusión	15	39	97	26	14
Fraude	8	13	66	41	78
Malware	75	311	387	200	166
SPAM	0	8	21	0	0
Disponibilidad	10	28	55	54	12
Intento de intrusión	7	24	159	9	7
Robos de información	2	1	1	7	8
Contenido Abusivo				11	6
Recolección de información				111	1
Sistema Vulnerable				224	514
Otros	13	55	99	39	12

Ilustración 4 - Incidentes gestionados con relación a infraestructuras críticas[10]

[10] Informe: Estudio sobre la cibercriminalidad ed.2019, pg.33, Ministerio del Interior

Sector estratégico	INCIDENTES GESTIONADOS				
	2015	2016	2017	2018	2019
Energía	46	126	213	149	151
Transporte	24	90	152	192	197
Tecnologías Informac. y Comunicac. (TIC)	17	17	40	46	50
Sistema tributario y financiero	17	152	250	214	266
Alimentación	12	47	42	40	57
Agua	5	40	134	57	64
Industria nuclear	5	4	12	5	18
Administración	1	2	10	1	0
Espacio	0	0	1	3	4
Industria química	0	0	0	15	11
Instalaciones de Investigación	0	0	0	0	0
Salud	0	0	1	0	0
Todos los sectores afectados	3	1	0	0	0

Ilustración 5 - Incidentes gestionados por sector estratégico[11]

En las dos tablas anteriores podemos ver las investigaciones reportadas de diferentes infraestructuras críticas de estado por tipo de incidente y por sector. Estas sugieren que las capacidades de detección respecto al resto de investigaciones analizadas por el CERT de infraestructuras no críticas son similares en proporción de incidentes reportados por tipo.

Es muy probable que muchos de los incidentes de seguridad no se reporten salvo que exista un requerimiento legal por ejemplo cuando una incidente escala a brecha de seguridad. No obstante, esta conjetura no es posible contrastarla ya que solo se analiza información agregada.

Si analizamos la tabla de investigaciones reportadas por sector estratégico los datos sugieren que algunos sectores o bien tienen menor capacidad de detección o bien no están reportando información a su CERT de referencia. Por ejemplo, el sector de la salud o industria química.

Este tipo de afirmaciones, al no poder ser contrastadas con datos por la ausencia de estos deberían ser cuestionadas. El problema para cuestionar es generalizado y cuenta con dos puntos de vista a tratar. El primer punto de vista es el de aquellas amenazas detectadas y no reportadas. El segundo punto es el de las amenazas que se han producido y no han sido detectadas ya sea por falta de medios o por el nivel de complejidad de la propia amenaza. Se debería abrir un debate en torno a como deberían las organizaciones públicas y privadas colaborar para mejorar su postura de ciberseguridad y como deberían realizarse estas acciones de colaboración entre los diferentes organismos para que se hagan efectivas estas mejoras.

Centro Criptológico Nacional Computer Emergency Response Team

¿Quiénes son?

El Centro Criptológico Nacional Computer Emergency Response Team, también conocido por su sigla CCN–CERT, es el organismo español, creado en 2006, encargado de contribuir a la ciberseguridad de la administración pública, los organismos públicos y empresas estratégicas

[11] Informe: Estudio sobre la cibercriminalidad ed.2019, pg.34, Ministerio del Interior

del país. CCN-CERT depende directamente del Centro Criptológico Nacional, del que toma parte de su nombre.[12]

¿Cómo nos ofrecen la información?

Mediante diferentes informes de carácter público. Durante el transcurso del proyecto se ha tratado de establecer contacto con la organización de forma no efectiva.

Cuentan con varias guías de fácil comprensión, que ayudan a mejorar la postura de ciberseguridad de las empresas e indican como actuar frente a diferentes tipos de incidentes. Estas guías pueden servir para construir casos de uso coherentes que traten los diferentes tipos de amenazas. También cuentan con estudios de interés en materia de ciberseguridad.

Ha sido objeto de análisis para el proyecto la última versión publicada en septiembre de 2020 del informe de ciberamenzas y tendencias incluido en el apartado de bibliografía.

El informe que realiza se basa en datos que no necesariamente provienen de las administraciones u organismo públicos y se apoya en publicaciones con citas como la siguiente las cual ha sido revisada e incluida en el proyecto.

"Al igual que en años anteriores, las brechas de datos continúan siendo habituales, y el 25% de las mismas estarían relacionadas con el espionaje, según asegura el Verizon Data Breach Investigation Report (DBIR) 2019. Dicho informe está basado en el análisis de 41.686 incidentes de seguridad, de los cuales 2013 se confirmaron como brechas de datos. Según el estudio, el 34 % de estas brechas está relacionado con actores internos, el 39% con organizaciones criminales y en el 23% de los casos las figuras responsables fueron Estados."[13]

Además, el mismo informe cuenta con un apartado de métodos de ataque donde explica con un nivel de detalle más avanzado las diferentes familias de amenazas que existe como por ejemplo los diferentes tipos de ransomware que existen como Dridex, Emotet.

A continuación, se presenta una clasificación no orientada al delito si no al tipo de ataque extraída del informe la cual se aproxima más a los diferentes tipos de amenazas desde un punto de vista técnico.

1. Actividades de ransomware
2. Botnets
3. Código dañino avanzado

[12] Web: Wikipedia, (28 de 12 de 2021) https://es.wikipedia.org/wiki/Centro_Criptol%C3%B3gico_Nacional_Computer_Emergency_Response_Team

[13] Informe: Ciberamenazas y tendencias ed.2020, pg.25, Centro Criptológico Nacional

4. Ataques a sistemas de acceso remoto
5. Ataques web
6. Ingeniería social
7. Ataques contra la cadena de suministro
8. Ataques contra sistemas ciberfísicos

Dirección General de Coordinación y Estudios

¿Quiénes son?

La Dirección General de Coordinación y Estudios es el órgano de apoyo y asesoramiento a través del cual la persona titular de la Secretaría de Estado de Seguridad ejerce su función de coordinación y supervisión de la actuación de las Fuerzas y Cuerpos de Seguridad del Estado y de colaboración con las policías autonómicas y las policías locales. Es el encargado de confeccionar las instrucciones y los planes directores y operativos de la Secretaría de Estado en materia de seguridad ciudadana, supervisando su ejecución; de elaborar periódicamente los datos estadísticos de criminalidad.[14]

¿Cómo nos ofrecen la información?

Nos ofrece un portal desde el cual podemos acceder a la información ya clasificada en base a diferentes criterios. Hasta el momento es el origen de datos más actualizado, contiene información actualizada hasta la fecha 29 de octubre del 2021 relacionada con el proyecto.

En el caso de que nos ocupa hemos extraído la información asociada a hechos conocidos de infracciones penales relacionadas con cibercriminalidad por grupo penal.

PORTAL ESTADÍSTICO DE CRIMINALIDAD

Series anuales. Cibercriminalidad. Comunidades y Ciudades Autónomas

Hechos conocidos de infracciones penales relacionadas con la cibercriminalidad por comunidades autónomas, grupo penal y periodo.

Unidades: hechos conocidos

	2020	2019	2018	2017	2016	2015	2014	2013	2012	2011
TOTAL NACIONAL										
ACCESO E INTERCEPTACIÓN ILÍCITA	4.653	4.004	3.384	3.150	3.243	2.893	1.851	1.805	1.701	1.492
AMENAZAS Y COACCIONES	14.066	12.782	12.800	11.812	12.036	10.607	9.559	9.064	9.207	9.839
CONTRA EL HONOR	1.550	1.422	1.448	1.561	1.546	2.205	2.212	1.963	1.891	1.941
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	125	197	232	121	129	172	183	172	144	222
DELITOS SEXUALES	1.783	1.774	1.581	1.392	1.231	1.306	974	768	715	755
FALSIFICACIÓN INFORMÁTICA	6.289	4.275	3.436	3.280	3.017	2.644	1.874	1.608	1.625	1.860
FRAUDE INFORMÁTICO	257.907	192.375	136.656	94.792	70.178	62.038	32.842	26.664	27.231	21.075
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	1.590	1.473	1.192	1.291	1.336	1.193	440	359	298	228
TOTAL grupo penal	287.963	218.302	160.729	117.399	92.716	83.058	49.935	42.403	42.812	37.412

Ilustración 6 - Infracciones penales relacionadas con cibercriminalidad

La siguiente tabla contrasta con los datos ofrecidos en los estudios revisados en organismos anteriores. A continuación, se ofrece de forma legible la información asociada a los últimos 3 años y nuevamente los datos de 2019 coinciden con las fuentes anteriores.

Total Nacional	2020	2019	2018
Acceso e interceptación ilícita	4.653	4.004	3.384

[14] Web: Ministerio del interior, (28 de 12 de 2021) http://www.interior.gob.es/el-ministerio/funciones-y-estructura/secretaria-de-estado-de-seguridad/direccion-general-de-coordinacion-y-estudios

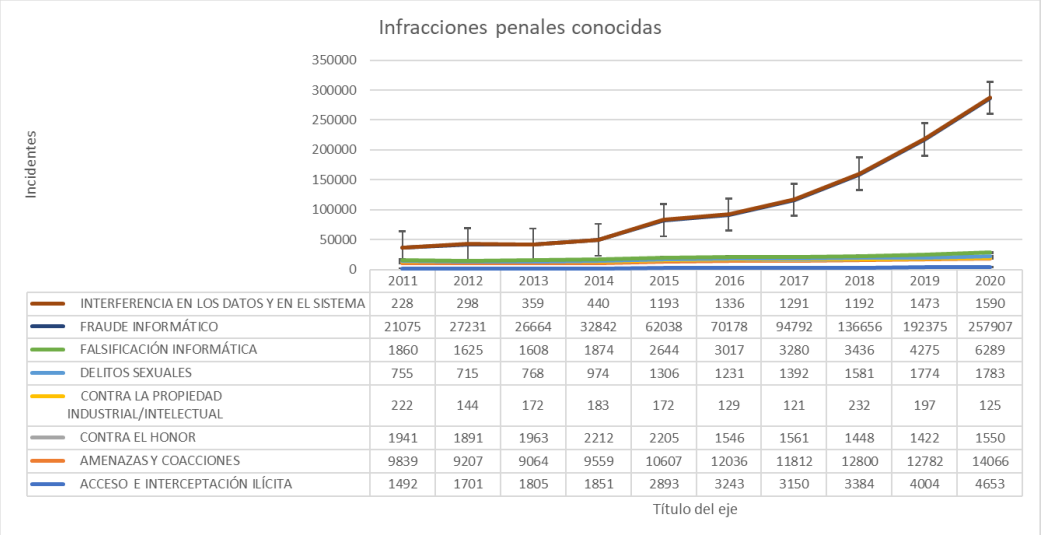
Amenazas y coacciones	14.066	12.782	12.800
Contra el honor	1.550	1.422	1.448
Contra la propiedad industrial/intelectual	125	197	232
Delitos sexuales	1.783	1.774	1.581
Falsificación informática	6.289	4.275	3.436
Fraude informático	257.907	192.375	136.656
Interferencia en los datos y en el sistema	1.590	1.473	1.192
TOTAL grupo penal	**287.963**	**218.302**	**160.729**

Tabla 21 - Historial estadísticas ciberdelitos en España

Aprovechando la información que se ofrece, se ha tratado de establecer las tendencias en el aumento de los incidentes reportados a lo largo de los años desde 2011.

Las siguientes líneas se han generado a partir de la información descargada del portal y se podrán ver en detalle en el fichero Excel adjunto a los entregables de la fase en curso.

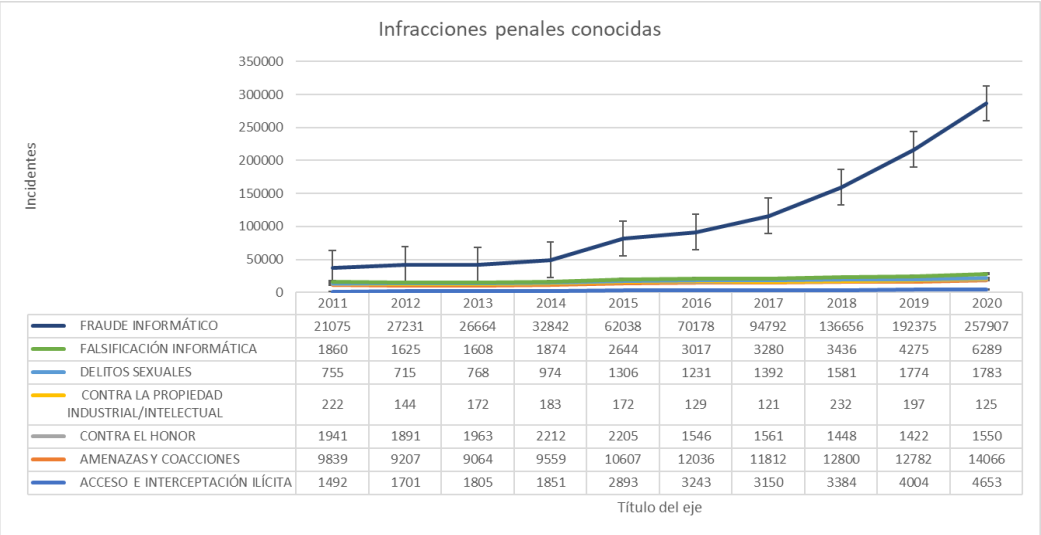
El primer gráfico muestra la tendencia al alza de los incidentes relativos a la inferencia de los datos y los sistemas.



	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA	228	298	359	440	1193	1336	1291	1192	1473	1590
FRAUDE INFORMÁTICO	21075	27231	26664	32842	62038	70178	94792	136656	192375	257907
FALSIFICACIÓN INFORMÁTICA	1860	1625	1608	1874	2644	3017	3280	3436	4275	6289
DELITOS SEXUALES	755	715	768	974	1306	1231	1392	1581	1774	1783
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	222	144	172	183	172	129	121	232	197	125
CONTRA EL HONOR	1941	1891	1963	2212	2205	1546	1561	1448	1422	1550
AMENAZAS Y COACCIONES	9839	9207	9064	9559	10607	12036	11812	12800	12782	14066
ACCESO E INTERCEPTACIÓN ILÍCITA	1492	1701	1805	1851	2893	3243	3150	3384	4004	4653

Ilustración 7 - Visión global infracciones penales conocidas I

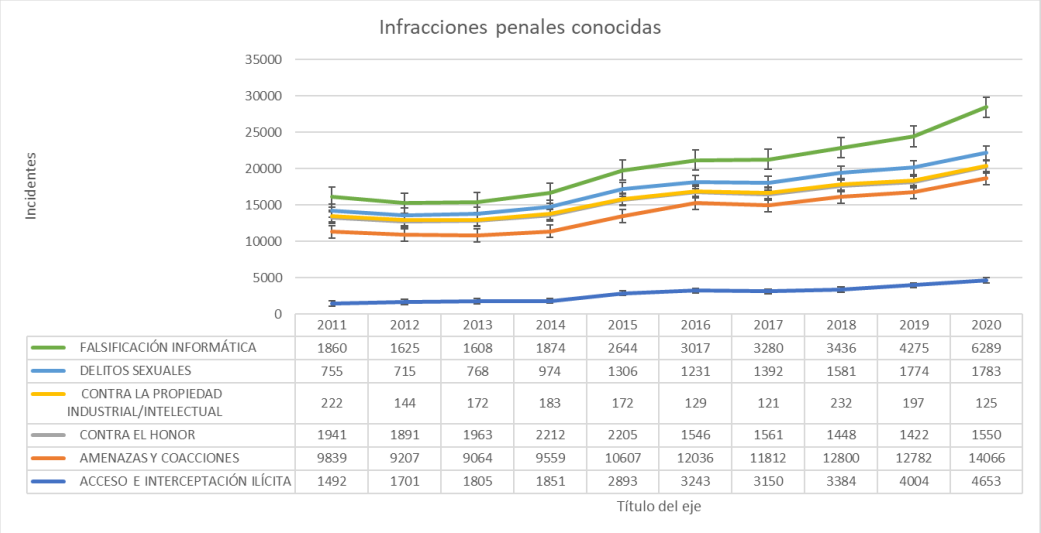
Con el objetivo de ampliar el foco se ha filtrado la categoría inferencia en los datos y sistemas. Se puede observar que el fraude se encuentra en segunda posición con un aumento relevante a lo largo de los años.



	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
FRAUDE INFORMÁTICO	21075	27231	26664	32842	62038	70178	94792	136656	192375	257907
FALSIFICACIÓN INFORMÁTICA	1860	1625	1608	1874	2644	3017	3280	3436	4275	6289
DELITOS SEXUALES	755	715	768	974	1306	1231	1392	1581	1774	1783
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	222	144	172	183	172	129	121	232	197	125
CONTRA EL HONOR	1941	1891	1963	2212	2205	1546	1561	1448	1422	1550
AMENAZAS Y COACCIONES	9839	9207	9064	9559	10607	12036	11812	12800	12782	14066
ACCESO E INTERCEPTACIÓN ILÍCITA	1492	1701	1805	1851	2893	3243	3150	3384	4004	4653

Ilustración 8 - Visión global infracciones penales conocidas II

Finalmente se realiza una nueva ampliación filtrando adicionalmente la categoría Fraude informático. Se puede aprecia que el resto de las categorías han aumentado ligeramente a lo largo de los años.



	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
FALSIFICACIÓN INFORMÁTICA	1860	1625	1608	1874	2644	3017	3280	3436	4275	6289
DELITOS SEXUALES	755	715	768	974	1306	1231	1392	1581	1774	1783
CONTRA LA PROPIEDAD INDUSTRIAL/INTELECTUAL	222	144	172	183	172	129	121	232	197	125
CONTRA EL HONOR	1941	1891	1963	2212	2205	1546	1561	1448	1422	1550
AMENAZAS Y COACCIONES	9839	9207	9064	9559	10607	12036	11812	12800	12782	14066
ACCESO E INTERCEPTACIÓN ILÍCITA	1492	1701	1805	1851	2893	3243	3150	3384	4004	4653

Ilustración 9 - Visión global infracciones penales conocidas III

2.1.2. Conclusiones obtención datos organizaciones

De las principales fuentes relacionadas con información de organismos públicos que aparecen en la redacción del proyecto se hará uso de los siguientes puntos para tratar de incluirlos en la prueba de concepto

- Observatorio Nacional de Tecnología y Sociedad
  - Su información no ha sido considerada para la ejecución de la fase de diseño y POC

- Observatorio Español de Delitos Informáticos

        - Modelo de clasificación basado en los diferentes tipos de ciberdelitos según la legislación.

- Ministerio del Interior
    - Se contemplará el top3 tanto por mayor volumen de notificaciones de incidentes como por menor volumen para incluir en los casos de uso de la POC.

- Centro Criptológico Nacional Computer Emergency Response Team
    - Las guías que ofrecen se utilizarán como referencia para idear los incidentes de seguridad y su tratamiento en la POC.

- Dirección General de Coordinación y Estudios
    - Nos ha permitido visualizar líneas de tendencia y contrastar que la información de los diferentes entes públicos utiliza el mismo origen de datos. No obstante, los criterios de clasificación tienen una orientación de carácter Penal y solo sobre los hechos reportados. Esto infiere que una parte importante de lo que está sucediendo no se está contemplando. Además, por la idiosincrasia de este tipo de amenazas, salvo excepciones como el hacktivismo y/o terrorismo, actividades que pueden buscar cierta notoriedad y repercusión mediática; el resto de las amenazas tratan de pasar en muchas ocasiones desapercibidas, tratando de eliminar cualquier rastro.
    - El análisis de datos y tendencias permitirá enriquecer las conclusiones.

2.1.3. Obtención información fuentes públicas

Para realizar esta parte del estudio se ha reducido la búsqueda realizada a una de las iniciativas más interesantes en lo que refiere a ciberamenzas detectadas por diferentes organismos y fabricantes.

DBIR 2021 Data Breach Investigation Report realizado por Verizon y referenciada en el apartado de bibliografía

Verizon Communications, Inc

¿Quiénes son?
Verizon Communications, Inc. (NYSE: VZ) es una compañía global de banda ancha y telecomunicaciones y parte del Índice Dow Jones.[15]

[15]Web: Wikipedia, (28 de 12 de 2021)
https://es.wikipedia.org/wiki/Verizon_Communications

¿Por qué Verizon?

Verizon nos ofrece una colección de enlaces donde colaborar y conocer cómo funciona su sistema de registro abierto de incidentes.

- github.com/vz-risk/dbir/tree/gh-pages/2021 (Incluye DBIR hechos, cifras y datos de cifras.)
- veriscommunity.net (Características información sobre un framework con ejemplos y listados de enumeración.)
- github.com/vz-risk/veris (Acceso a las características el esquema VERIS completo.)
- github.com/vz-risk/vcdb (Proporciona acceso a una base de datos de brechas de seguridad.)

Además, permite registrar nuestros propios incidentes de seguridad de forma anónima.

Esta es una de las mejores fuentes de información ya que cuenta con un método y desarrollos que respaldan su uso. Su terminología y métodos de clasificación nos permite tener una foto lo más cercana a los diferentes tipos de incidentes.

¿Cómo nos ofrecen la información?

Existe un repositorio git y diferentes métodos para poder extraer la información mediante diferentes scripts. También existe la posibilidad de extraer la información ya tratada la cual ha sido la opción utilizada.

A continuación, se presenta un ejemplo de lo que podemos encontrar en su informe o bien en su repositorio.

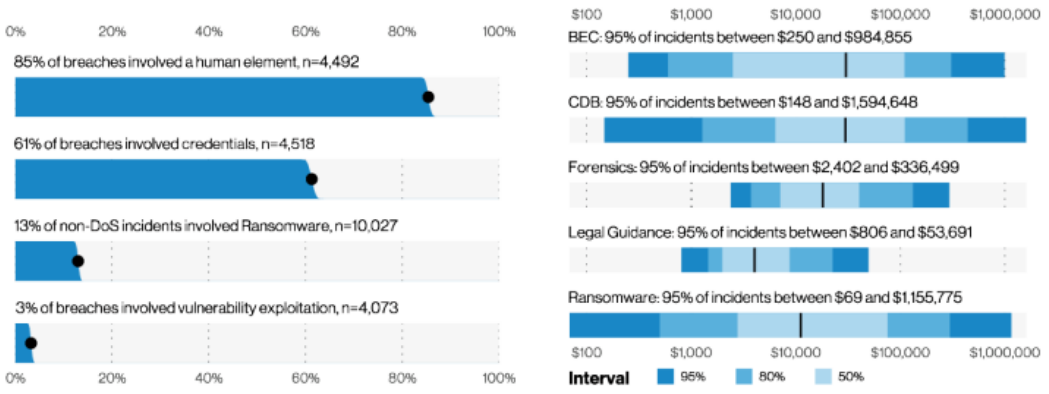


Figure 7. Select action varieties (n=4,073)

Figure 8. Select impacts of incidents

Ilustración 10 - Visión global informe Verizon[16]

El proyecto afirma que con el tiempo se convertirá en una fuente de datos rica y de libre acceso para realizar este tipo de investigación ad hoc.

[16] Informe: DBIR Data breach investigations report ed.2021, pg.7, Verizon

También afirma que regularmente reciben consultas sobre su conjunto de datos y opciones para compartir más información, pero indican que están limitados en cuanto a qué datos pueden compartir en formato sin procesar debido a los acuerdos con sus socios y clientes.[17]

A continuación, listamos los diferentes tipos de ataque los cuales mantiene cierta similitud con los que nos proponen el CCN-CERT o bien diferentes organizaciones como EC-Council, ISC2, SANS entre otras extraídas del informe de Verizon.

Tipología de ataques extraídas del informe:

- Social Engineering
- Basic Web Application Attacks
- System Intrusion
- Miscellaneous Errors
- Privilege Misuse
- Lost and Stolen Assets
- Denial of Service
- Everything Else

A continuación, podemos observar dos gráficas que no ayudarán a definir qué tipos de casos de uso realizar desde otro punto de vista.

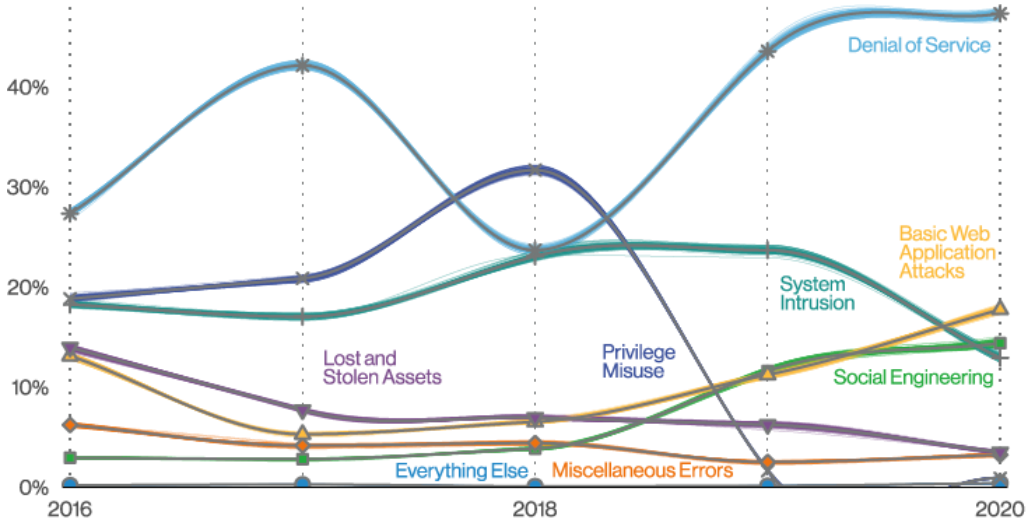


Ilustración 11 - Patrones de incidentes en tiempo[18]

[17] Web: Verizon, (28 de 12 de 2021) https://veriscommunity.net/vcdb.html

[18] Informe: DBIR Data breach investigations report ed.2021, pg.30, Verizon

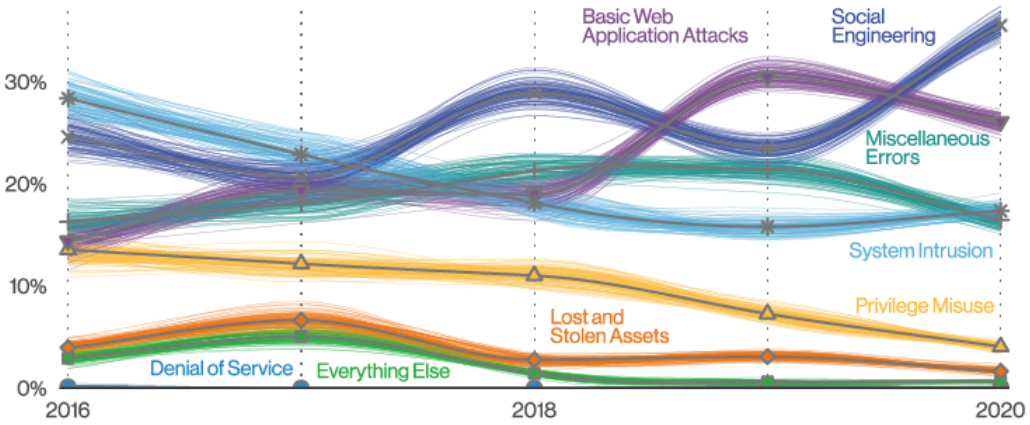


Ilustración 12 - Patrones de brechas en tiempo[19]

Importante una denegación de servicio implica una falta de disponibilidad, pero no una exposición de datos, eso explica su valor nulo en la gráfica de brechas de seguridad

Las siguientes tablas de datos han sido extraídas del informe y en algunos casos adaptadas para ayudar en la toma de decisiones a la hora de plantear los casos de uso.

Frecuencia			
	Incidentes	Brechas	Porcentaje de acierto
Denial of Service	14.335	4	0%
Lost and Stolen Assets	1.295	84	6%
Miscellaneous Errors	919	896	97%
Privilege Misuse	265	222	84%
Social Engineering	3.841	1767	46%
System Intrusion	3.710	966	26%
Basic Web Application Attacks	4.862	1384	28%
Everything Else	129	38	29%

Tabla 22 - Incidentes que derivan en brecha de seguridad (estudio Verizon)

En la tabla anterior podemos observar la cantidad de incidentes reportados y cuantos derivan en brecha de seguridad. Se ha de destacar que los ataques de ingeniería social junto con el uso inadecuado de privilegios tienen unos porcentajes de acierto elevados. Desafortunadamente no se han incluido los ataques de ingeniería social como parte de la POC por la variedad de estos. Además, no siempre se realizan los ataques de ingeniería social en entornos tecnológicos. Se ha valorado la realización de un caso de uso de phishing para cubrir un posible incidente de ingeniería social. No obstante, ejercicios de concienciación en las personas puede cubrir un alcance más amplio sobre las diferentes fórmulas de ataque que se pueden dar y por este motivo se ha descartado de la POC.

[19] Informe: DBIR Data breach investigations report ed.2021, pg.30, Verizon

Threat Actors				
	External	Internal	Multiple	Partner
Denial of Service				
Lost and Stolen Assets	79%	15%	5%	1%
Miscellaneous Errors	0%	98%	1%	1%
Privilege Misuse	7%	84%	8%	2%
Social Engineering	100%	0%	0%	0%
System Intrusion	91%	8%	1%	0%
Basic Web Application Attacks	98%	1%	1%	0%
Everything Else	95%	5%	0%	0%

Tabla 23 - Incidentes por tipo de actor e incidente (estudio Verizon)

Respecto a los diferentes tipos de actores en una gran mayoría de casos son externos y se ha tenido en consideración para montar los casos. Para ello se ha contemplado en uno de los casos uso un firewall perimetral para detectar amenazas realizadas por posibles actores externos.

Actor Motives						
	Financial	Fun	Espionage	Grudge	Convenience	Ideology
Denial of Service	0%	0%	0%	0%	0%	0%
Lost and Stolen Assets	100%	0%	0%	0%	0%	0%
Miscellaneous Errors	0%	0%	0%	0%	0%	0%
Privilege Misuse	59%	16%	8%	13%	3%	1%
Social Engineering	94%	0%	6%	0%	0%	0%
System Intrusion	94%	0%	6%	0%	0%	0%
Basic Web Application Attacks	90%	1%	7%	2%	0%	0%
Everything Else	100%	0%	0%	0%	0%	0%

Tabla 24 - Incidentes por motivo de actores e incidente (estudio Verizon)

Los motivos simplemente se utilizarán para contextualizar las amenazas. No obstante, el factor más relevante es el económico según la información obtenida del estudio.

Data Compromised							
	Personal	Medical	Bank	Other	Credentials	Internal	Payment
Denial of Service	0%	0%	0%	0%	0%	0%	0%
Lost and Stolen Assets	58%	31%	6%	5%	0%	0%	0%
Miscellaneous Errors	59%	13%	10%	10%	10%	0%	0%
Privilege Misuse	44%	19%	0%	24%	0%	13%	0%
Social Engineering	15%	3%	0%	8%	74%	0%	0%
System Intrusion	34%	0%	0%	25%	24%	0%	17%
Basic Web Application Attacks	31%	0%	0%	15%	47%	7%	0%
Everything Else	0%	0%	0%	0%	0%	0%	100%

Tabla 25 - Incidentes por dato comprometido e incidente (estudio Verizon)

Finalmente se han extraído los porcentajes sobre los diferentes tipos de información extraídos en base a cada tipo de ataque lo cual ayudará a contextualizar los casos de uso. De forma concreta uno de los casos de uso contemplará información de credenciales robadas uno de los elementos más relevantes respecto a la información comprometida.

2.1.4. Conclusiones obtención información fuentes públicas

De la principal fuente analizada que no representa a ningún organismo público se hará uso de los siguientes puntos para tratar de incluirlos en la POC

- Verizon Communications, Inc
    - Se contemplará el tipo de dato filtrado más relevante que son las credenciales.
    - El análisis de datos y tendencias permitirá enriquecer las conclusiones.

2.2. Estudio de los datos

El apartado definido como estudio de los casos de uso pasará a ser una propuesta sobre la temática de las amenazas a tratar mediante la siguiente aproximación.

Incluir uno o dos casos de uso que incluyan las siguientes tipologías de ciberamenzas de mayor volumen reportado

- Fraude
- Sistemas vulnerables
- Malware

Incluir un caso de uso que incluya una de las siguientes tipologías de ciberamenzas de menor volumen reportado.

- Disponibilidad
- Recolección de información
- Intento de intrusión

Incluir un sistema de clasificación que permita determinar si la investigación en curso pertenece a una de las siguientes categorías, independiente del tipo de ataque o ataques identificados durante la investigación en curso.

- Acceso e interceptación ilícita
- Interferencia en los datos y en el sistema
- Falsificación informática

- Fraude Informático
- Delitos sexuales
- Contra la propiedad industrial intelectual
- Contra el honor
- Delitos contra la salud pública
- Amenazas y coacciones

2.3. Determinar criterios de selección

Para determinar un criterio de selección basado en los tipos de amenazas o bien tipo de delito informático, es necesario conocer el riesgo y el impacto que suponen las diferentes amenazas que han sido reportadas.

Al no contar con este tipo de información no se puede establecer un criterio sólido que no se base en contar cantidad de incidentes reportados.

A modo de ejemplo desconocemos si los fraudes reportados se han consumado o no y bien cuál ha sido o ha podido ser el impacto y el alcance de estos.

Un breve adelanto sobre las conclusiones es que es necesario un método de clasificación de incidentes aceptado y utilizado por todo el sector tecnológico. Un símil sería el sistema de clasificación utilizado para identificar las vulnerabilidades que ofrece MITRE con sus conocidos CVE. De la misma forma sería necesario un sistema que permita a las diferentes organizaciones compartir y colaborar de forma que estas se sientan cómodas. Abordar esta idea en un plano teórico podría ser objeto de un TFM completo.

Por lo tanto, podemos concluir que no es posible determinar un criterio solido basado en los conjuntos de datos de información agregada que se facilitan en los diferentes informes analizados.

3. Diseño y POC

En la Entrega de la asociada al hito Entrega 2 se indicó que tentativamente se tratarían de cubrir los siguientes tipos de casos de uso como resultado del estudio realizado.

Esta es la primera aproximación que fue propuesta de casos de uso a resolver en la POC.

Incluir uno o dos casos de uso que incluyan las siguientes tipologías de ciberamenzas de mayor volumen reportado

- Fraude
- Sistemas vulnerables
- Malware

Incluir un caso de uso que incluya una de las siguientes tipologías de ciberamenzas de menor volumen reportado.

- Disponibilidad
- Recolección de información
- Intento de intrusión

Incluir un sistema de clasificación personalizado que permita registrar si el incidente en curso o tratado se clasifica según un sistema de clasificación con base en el código penal español.

Como resultado final de las ideas tentativas se ha realizado el diseño de tres casos de uso y un sistema de clasificación:

- Caso de uso de malware (C2)
- Caso de uso de robo de credenciales (Data Leak)
- Caso de uso de acceso no autorizado (Fuerza Bruta)
- Sistema de clasificación según tipificación utilizada por el estado

Por lo tanto, queda cubierto un caso de malware, un caso de recolección de información y un caso de intento de intrusión.

3.1. Herramienta SOAR

Para realizar la prueba de concepto se ha seleccionado la herramienta Cortex XSOAR de Palo Alto Networks. Para ello ha sido necesario solicitar una versión de evaluación al fabricante.

Existen dos motivos principales por los cuales se ha seleccionado esta herramienta SOAR.

El motivo principal, es que cuenta con un gran número de integraciones con plataformas de terceros. Esto daría dinamismo y flexibilidad a la hora de implementar e idear los casos de uso sin condicionar el diseño de estos a la falta de integraciones o automatizaciones que requerirían desarrollo.

El segundo motivo es la usabilidad de la herramienta, la cual facilitaría la realización de los casos de uso y posibles modificaciones durante la implementación de los casos de uso.

Existen otros condicionantes, como el hecho de poder obtener de repositorios públicos del propio fabricante el código que se ejecuta en cada una de las automatizaciones e integraciones. Con este código se podrían llegar a programar con relativa facilidad los casos de uso con un IDE de desarrollo para después ponerlos en producción. Aunque se perdería toda la usabilidad sería perfectamente viable.

Cabe mencionar que existen muchas funciones avanzadas de las que no se ha hecho uso. El motivo es que se pueda trasladar el trabajo realizado a cualquier otra herramienta SOAR del mercado sin que algún tipo de característica propia o avanzada de la herramienta suponga un impedimento.

3.2. Diseño de los casos de uso

Los siguientes apartados definirán los casos de uso que han sido implementados en la herramienta SOAR seleccionada para la prueba de concepto.

La definición del caso de uso define la lógica y las tareas que se realizan como parte de un proceso de respuesta a incidentes para un tipo de incidente específico.

Los tres casos de uso propuestos cuentan cada uno con un tipo de incidente y un playbook principal asociado como se puede ver en la siguiente tabla capturada directamente de la aplicación.

Tipo	Playbook
C2	Malware (C2) - core
Data Leak	Robo de credenciales (Data Leak) - core
Fuerza Bruta	Acceso no autorizado (Fuerza Bruta) - core

Tabla 26 - Tipos de incidentes y playbooks

Para trata cada uno de los casos de uso se ha optado por utilizar un tipo de disparador diferente con el objetivo de poner a prueba las capacidades de la herramienta SOAR.

- Disparador integración splunk

Para el caso de uso de “fuerza bruta” la herramienta SOAR realizará cada minuto una petición para traer todos los registros asociados a intentos de acceso fallidos superiores a 3 por minuto. Esto abrirá una investigación y ejecutará de forma automática el playbook asociado.

- Servidor de syslog integrado en XSOAR

  El orquestador está a la espera de recibir un mensaje de syslog. El sistema solo acepta mensajes de syslog de un firewall perimetral el cual ha sido preconfigurado solo para enviar mensajes en caso de detectar una petición hacia internet a una IP previamente categorizada como maliciosa.

Los dos casos anteriores han requerido de una configuración especifica de clasificación y mapeado de campos para la correcta ejecución de los playbooks diseñados.

- Tarea programada que ejecuta un playbook

  Para el caso de uso de “robo de credenciales” se ha dispuesto un playbook que de forma periódica verifica la existencia de credenciales robadas asociadas a un email de usuarios considerados críticos como VIP y administradores de sistemas en base a la información de un controlador de dominio.

- Ejecución manual

  El playbook de “robo de credenciales” contempla posibilidades de ejecución manual mediante un playbook previo asistido que presenta un formulario a completar por un analista.

- Ejecución por email

  El playbook de “robo de credenciales” contempla posibilidades de ejecución mediante él envió de un mail a un buzón gestionado por el SOAR. Una vez procesado el mail se extraen todas las direcciones de correo existente en el cuerpo del email.

A continuación, se presentará el diseño de los casos de uso mediante una ficha donde se redacta a alto nivel la lógica de los casos de uso que se han implementado durante la POC.

3.2.1. Caso de uso de malware (C2)

El caso de uso se ejecutará a partir de la recepción de un mensaje de syslog proveniente de un firewall perimetral que ha detectado una conexión a una IP maliciosa asociada a un Command & Control (C&C).

Este evento se enviará directamente a la herramienta SOAR para su tratamiento. En el caso de que la máquina de origen se encuentre en una whitelist de exclusión de acciones automáticas, se notificará al equipo responsable del activo para ampliar información sobre el suceso y servicio. Esta respuesta se facilitará al servicio de SOC para que determine las acciones más convenientes a realizar.

Por otro lado, en el caso de que se trate de un equipo virtualizado y no considerado activo crítico de negocio (ACN), automáticamente se procederá a la desconexión de las tarjetas de red. En el caso de que se trate de un ACN, se notificara por slack al SOC, para que determinen las acciones a realizar (Apagado del equipo y/o desconexión de tarjetas de red y/o snapshot) marcando las acciones en una checklist.

Finalmente se clasificará y cerrará la investigación.

3.2.1.1. Ficha

La siguiente ficha define los elementos más relevantes del caso de uso.

Caso de uso	**Malware (C2)**
Disparador	El caso de uso se ejecutará a partir de la recepción de una petición hacia una IP identificada como maliciosas en un firewall perimetral. En el caso de uso propuesto se enviará un mensaje de syslog directamente a la herramienta SOAR sin necesidad de hacer uso de un SIEM. Será el propio SOAR quien realice la gestión de eventos repetidos.
Estructura y mapeo de incidentes	Campos obligatorios: IP de origen. IP de destino.
Proceso de respuesta a incidentes	1. Si IP de origen de la petición al C&C está en whitelist de acciones automáticas, notificar a equipo responsable del equipo y solicitar explicaciones. En caso contrario: continuar con proceso. 2. Verificar si equipo es máquina virtual. Sí: Verificar sí es ACN. Sí: Notificar a equipo analistas para que determinen acciones a realizar (Apagar equipo/Realizar snapshot/Desconectar interfaces de red/Continuar el proceso). No: Desconectar tarjetas de red. No: Notificar al SOC. 3. Registrar anotaciones sobre la investigación. 4. Clasificar incidentes según legislación. 5. Cerrar investigación.

Enriquecimiento	Descartado enriquecimiento debido a que la IP ya ha sido categorizada previamente.
Pasos manuales	Tarea con comentarios manuales sobre el suceso del analista de SOC si el equipo no es virtual y no está en whitelist.
Interacción con usuario afectado o analista	Envío de mail a equipo responsable del activo en whitelist para que justifique el suceso. Envío de formulario de acciones a SOC para determinar acción a realizar.
Lógica de duplicación	Agrupar eventos con misma IP de Origen y misma IP de destino para investigaciones no cerradas. (Esto se realiza como parte del preprocesado paso previo a la creación de la investigación).

Tabla 27 - Caso de uso malware (C2)

3.2.1.2. Integraciones

El siguiente apartado indica las integraciones con plataformas externas a la herramienta SOAR que participarán en el proceso de orquestación y los comandos asociados a las acciones a realizar.

Nombre	Acciones necesarias
AnsibleVMware	vmware-guest-info
Mail Sender	send-mail
Salck	send-notification
Syslog	fetch
VMware	vmware-change-nic-state vmware-create-snapshot vmware-get-vms vmware-poweroff

Tabla 28 - Integraciones caso de uso malware (C2)

3.2.1.3. Anotaciones

No se ha contemplado enriquecer información con la IP de destino de C&C con información relevante para el SOC ya que se presupone que la IP ya ha sido categoriza previamente como maliciosa generando la alerta. El caso de uso podría ser ampliado tratando de buscar si anterior a la categorización han habido otras peticiones a la misma IP.

3.2.1.4. Vista diseño

La siguiente imagen ilustra el flujo del playbook principal que será ejecutado tras la recepción del mensaje de syslog en la herramienta SOAR. En la documentación anexa se pueden encontrar las imágenes

con mayor nivel de calidad, así como los desarrollos realizados y documentación técnica.

Playbook base

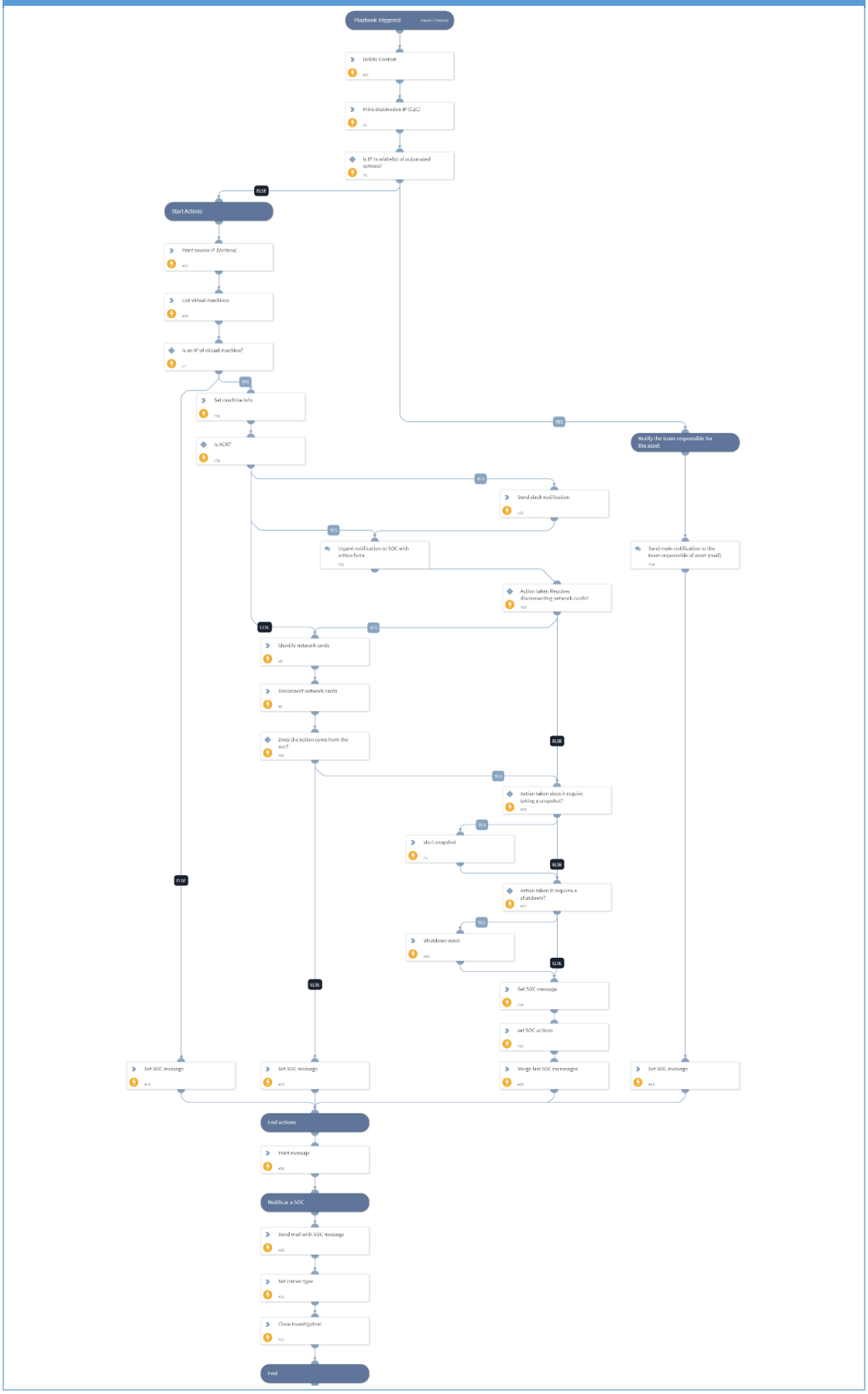


Tabla 29 - Playbook Malware (C2) - core

3.2.2. Caso de uso de robo de credenciales (Data Leak)

El siguiente caso de uso tiene como objetivo detectar credenciales filtradas de usuarios existentes y no rotadas anteriores a la fecha de filtración. Se hará uso del servicio “Have I been pwned” para obtener dicha información. Este playbook contará con 3 modos de ejecución diferentes.

El primero será mediante el uso de una tarea programada (job), que detectará los usuarios del directorio activo (AD) que pertenecen a un grupo de usuarios VIP y/o un grupo de usuarios administradores de sistemas. Con el listado de usuarios obtenido se realizará la verificación 1 a 1 de si existen credenciales filtradas.

El segundo modo de activación será mediante el envío de un email el cual extraerá y analizará todos los emails contenidos en el cuerpo del email.

El tercero será mediante la ejecución manual del playbook el cual solicitará que se introduzca el email o emails de usuarios a verificar.

En todos los casos se abrirá un incidente independiente a modo de ticket en la propia herramienta SOAR para su análisis detallado.

3.2.2.1. Ficha

La siguiente ficha define los elementos más relevantes del caso de uso.

Caso de uso	**Robo de credenciales (Data Leak)**
Disparador	El caso de uso se ejecutará de 3 formas diferentes. Job - Haciendo uso de una tarea programada. Manual - Mediante la creación de un caso directamente en la herramienta. Mail - Mediante el envío de un mail al buzón soaruoc@gmail.com el cual cuenta con una integración que gestiona los mails entrantes de forma automática.
Estructura y mapeo de incidentes	Campos obligatorios: Body.
Proceso de respuesta a incidentes	1.(job) Verificar grupos de AD para identificar usuarios VIP y Administradores de sistema. Extraer listado mails. 1.(manual) Abrir incidente manualmente y rellenar campo con email o emails a analizar. Extraer listado mails. 1.(mail) Enviar mail a buzón soaruoc@gmail.com con los mails que se desea analizar en el cuerpo del mensaje. Extraer listado mails. 2.Verificar si existen credenciales que han sido filtradas: Sí: Verificar si existe usuario en AD. Sí: Determinar si el leak es posterior a la última modificación de credenciales.

	Sí: Determinar se ha de abrir nueva investigación. Abrir investigación. No: Continuar. No: Continuar. No: Continuar. 3. Cerrar investigación.
Enriquecimiento	Se obtendrá información de cuentas que han sido filtradas y registradas en la herramienta “Have I been pwned”
Pasos manuales	No se requieren. La gestión del incidente se delegará al tratamiento de la investigación.
Interacción con usuario afectado o analista	Solo se requiere facilitar email en los casos de ejecución manual y por email.
Lógica de duplicación	No se requiere. El propio playbook es el encargado de determinar si existe investigación abierta sobre el mismo leak.

Tabla 30 - Caso de uso robo de credenciales (Data Leak)

3.2.2.2. Integraciones

El siguiente apartado indica las integraciones con plataformas externas a la herramienta SOAR que participarán en el proceso de orquestación y los comandos asociados a las acciones a realizar.

Categoría de producto	Acciones necesarias
Active Directory Query	ad-get-group-members ad-get-user
Have I Been Pwned	pwned-email
Mail Listener	fetch

Tabla 31 - Integraciones caso de uso robo de credenciales (Data Leak)

3.2.2.3. Anotaciones

La solución Have I been pwned no cuenta con timestamp que permita realzar búsqueda por fecha de filtrado del leak. Esto provoca que se tanga que controlar en la propia investigación si leak ya ha sido tratado, para evitar generar nuevas investigaciones duplicadas.

3.2.2.4. Vista diseño

La siguiente imagen ilustra el flujo del playbook principal que será ejecutado por cada uno de los mails que se introduzca como input. En la documentación anexa se pueden encontrar las imágenes con mayor nivel de calidad, así como los desarrollos realizados y documentación técnica.

Playbook base

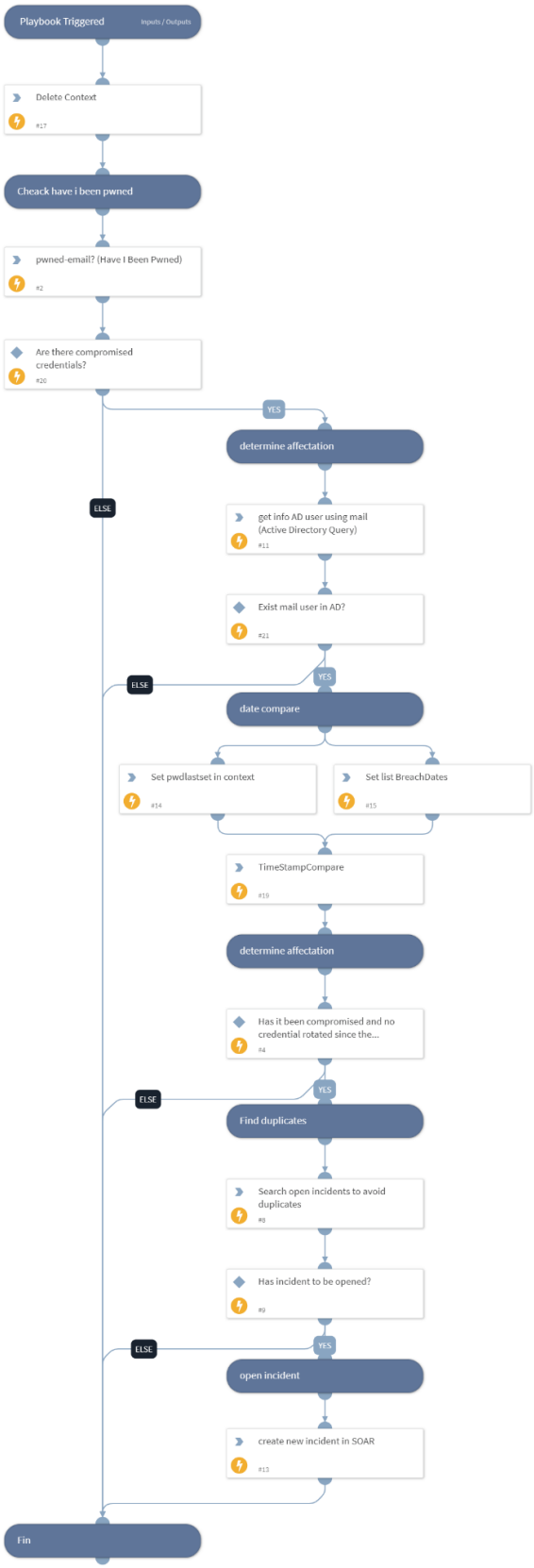


Tabla 32 - Playbook robo de credenciales (Data Leak) - core

A continuación, se presentan los diferentes playbooks que facilitan la ejecución del playbook base.

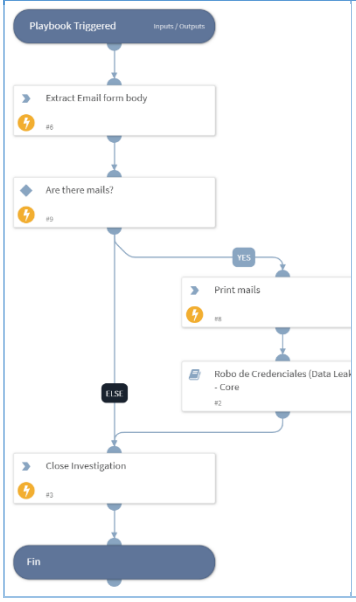
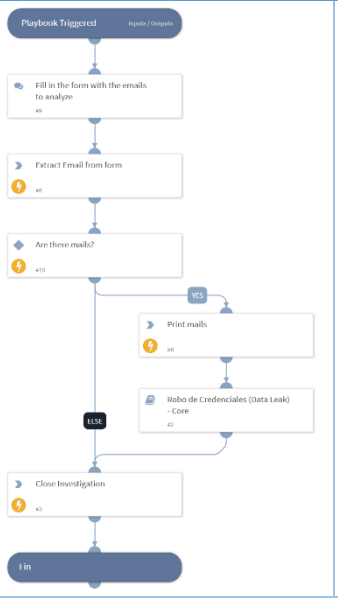
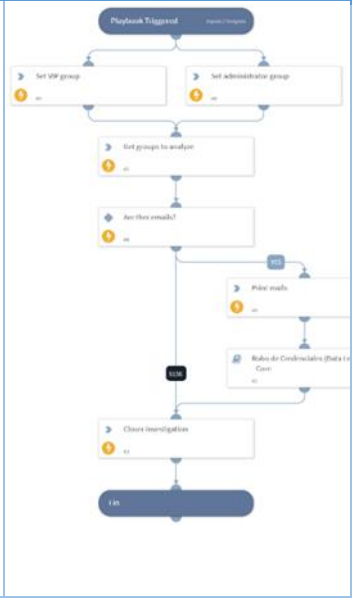
Accionado por mail	Accionado manual	Accionado con tarea programada
		

Tabla 33 - Playbook disparadores de robo de credenciales

3.2.3. Caso de uso de acceso no autorizado (Fuerza bruta)

El siguiente caso de uso tiene como objetivo tratar alertas de fuerza bruta utilizando como disparador un SIEM (Splunk). Con el uso de los eventos de seguridad generados por el controlador dominio se ha creado una alerta en el SIEM que detecta intentos de acceso fallidos (más de 3 en un minuto para la POC). Estos tendrán como origen un servidor “ftp” que solo permite accesos de usuarios dados de alta en el controlador de domino.

El playbook determinara si el ataque es de un usuario existente en el controlador de dominio y si existe la posibilidad de que la credencial se encuentre filtrada y activa.

En caso de que se cumplan todas las condiciones se notificará y solicitará la aprobación del SOC para un rotado automático de contraseña. En caso contrario simplemente se enviará notificación al SOC. En lo que refiere al usuario en caso de que se cuente con el teléfono registrado en el directorio activo, se le notificara por mail y mediante el envío de un SMS al teléfono.

Finalmente, la investigación será clasificada y cerrada.

3.2.3.1. Ficha

La siguiente ficha define los elementos más relevantes del caso de uso.

Caso de uso	Acceso no autorizado (Fuerza bruta)
Disparador	El caso de uso se ejecutará con la opción “fetch” que ingesta haciendo uso de la integración Splunk de la herramienta, obteniendo las nuevas alertas de seguridad registradas en el SIEM.
Estructura y mapeo de incidentes	Campos obligatorios: ComputerName. Usuario. Timestamp. Count.
Proceso de respuesta a incidentes	1. Identificar si el usuario detectado en el FTP existe en el AD, cuando fue el último rotado de credencial, mail y teléfono móvil. Sí: usuario existe: Determinar si el leak es anterior o posterior a la última modificación de credenciales. No: No hacer nada. 2. Determinar severidad: Low: Usuario no existe. Medium:Usuario existe, pero credenciales no comprometidas. High: Usuario existe, credencial comprometida y contraseña rotada Critical: Usuario existe, credencial filtrada y contraseña no rotada. 3. Acciones. 3.1 Notificar a SOC Sí: Severidad Critica Notificar a SOC por Slack Solicitar Acción Si: Acción seleccionada es Rotar credencial. Generar nueva credencial. Modificar credencial. Si: Acción es otra: Continuar playbook. Otra severidad: Continuar playbook. 3.2 Notificar a Usuario. Sí: Severidad critica. Notificar por mail y SMS. Sí: Severidad Alta.

	Notificar por mail a usuario con copia al SOC. Otra severidad: Continuar playbook. 4. Determinar clasificación del incidente. 5. Cerrar investigación.
Enriquecimiento	Se utilizarán como fuentes de enriquecimiento Have I been pwned para cuentas de usuario y el controlador de dominio.
Pasos manuales	No aplica.
Interacción con usuario afectado o analista	Solicitud de aprobación al SOC para rotado de contraseña.
Lógica de duplicación	Agrupar eventos con mismo usuario y tipo de incidente en estado abierto.

Tabla 34 - Caso de uso acceso no autorizado (Fuerza Bruta)

3.2.3.2. Integraciones

El siguiente apartado indica las integraciones con plataformas externas a la herramienta SOAR que participarán en el proceso de orquestación y los comandos asociados a las acciones a realizar.

Categoría de producto	Acciones necesarias
Active Directory Query	ad-get-user ad-set-new-password
Have I Been Pwned	pwned-email
Mail Sender	send-mail
Slack	send-notification
Twilo	TwilioSendSMS

Tabla 35 - Integraciones caso de uso acceso no autorizado (Fuerza bruta)

3.2.3.3. Anotaciones

Se podría forzar el rotado automático de credenciales para mitigar el riesgo sin validación por parte del SOC.

3.2.3.4. Vista diseño

La siguiente imagen ilustra el flujo del playbook principal que será ejecutado a partir de los logs de splunk desde la herramienta SOAR con una query predefinida. En la documentación anexa se pueden encontrar

las imágenes con mayor nivel de calidad, así como los desarrollos realizados y documentación técnica.

Playbook base

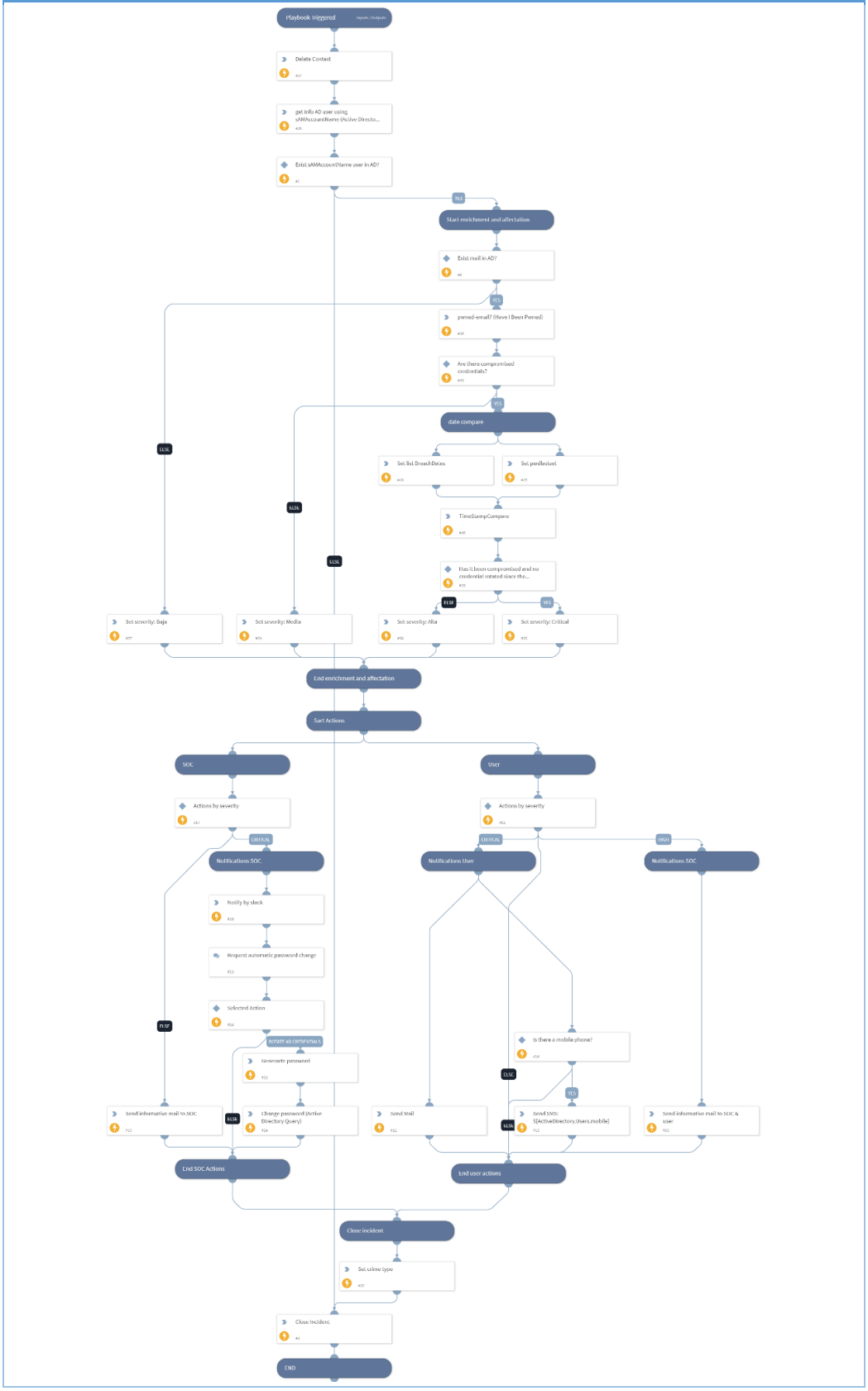


Tabla 36 - Playbook Acceso no autorizado (Fuerza bruta) - core

3.3. Sistema de clasificación según tipificación utilizada por el estado

Se ha implementado un sistema de clasificación que se permite categorizar una investigación según los tipos de incidentes definidos por el Ministerio del Interior de España. Aunque este sistema de clasificación de incidentes no es el más adecuado por diversas razones, nos permite poner a prueba la flexibilidad de las herramientas SOAR no solo como herramientas de orquestación si no como herramientas con capacidades avanzadas que permiten adaptarse a diferentes necesidades.

Para ello se ha añadido un campo personalizado a la herramienta, el cual ha sido indexado con el objetivo de poder explotar la información en reportes o dashboards. Al campo personalizado se le han configurado los siguientes valores:

- Acceso e interceptación ilícita
- Interferencia en los datos y en el sistema
- Falsificación informática
- Fraude Informático
- Delitos sexuales
- Contra la propiedad industrial intelectual
- Contra el honor
- Delitos contra la salud pública
- Amenazas y coacciones

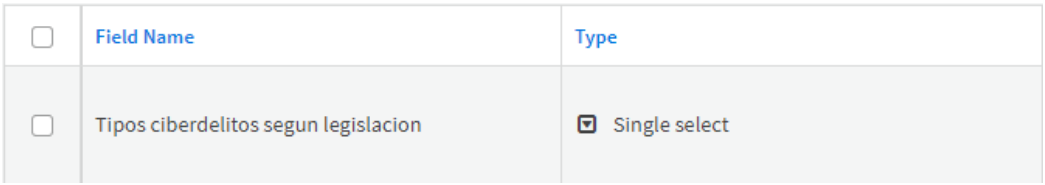


Ilustración 13 - Campo de clasificación personalizado

Con el objetivo de mejorar la usabilidad de la herramienta, se ha creado un automatismo, el cual evita el error humano al rellenar este campo en los playbooks como acción automática o investigaciones de forma manual y permite seleccionar durante la creación de un playbook solo los valores predefinidos de forma rápida.

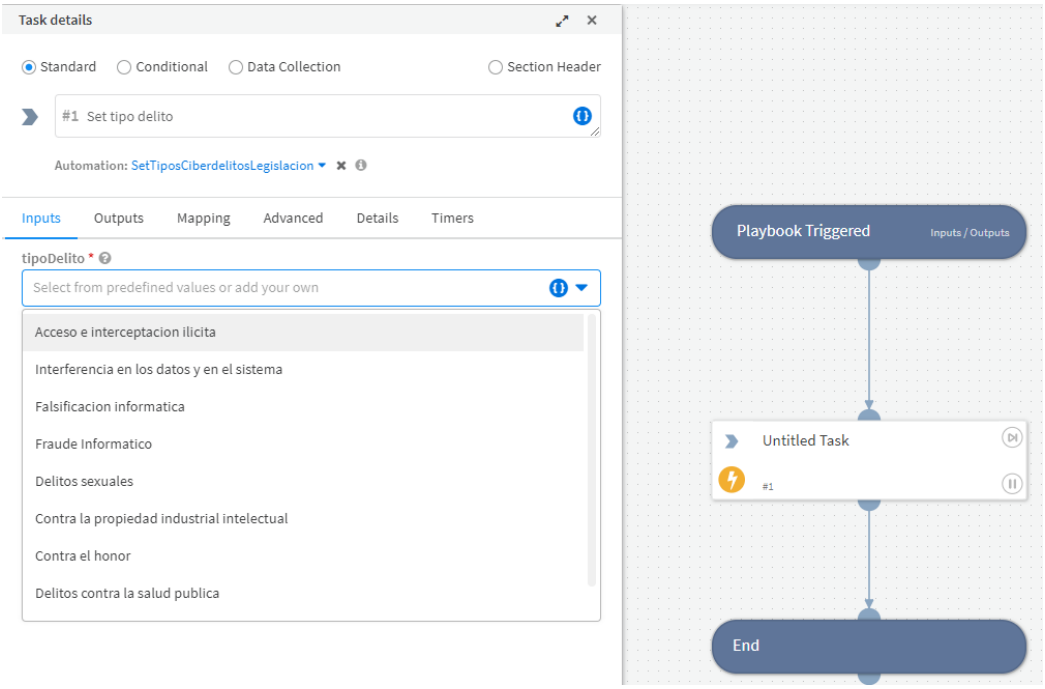


Ilustración 14 - Ejemplo de automatismo creado en diseño de un playbook

En la siguiente captura se puede visualizar de forma rápida el número de incidencias cerradas que han sido categorizadas según tipologías de delito en una línea de tiempo, a proporción con el resto de los tipos de incidentes y un acceso rápido a los mismos.

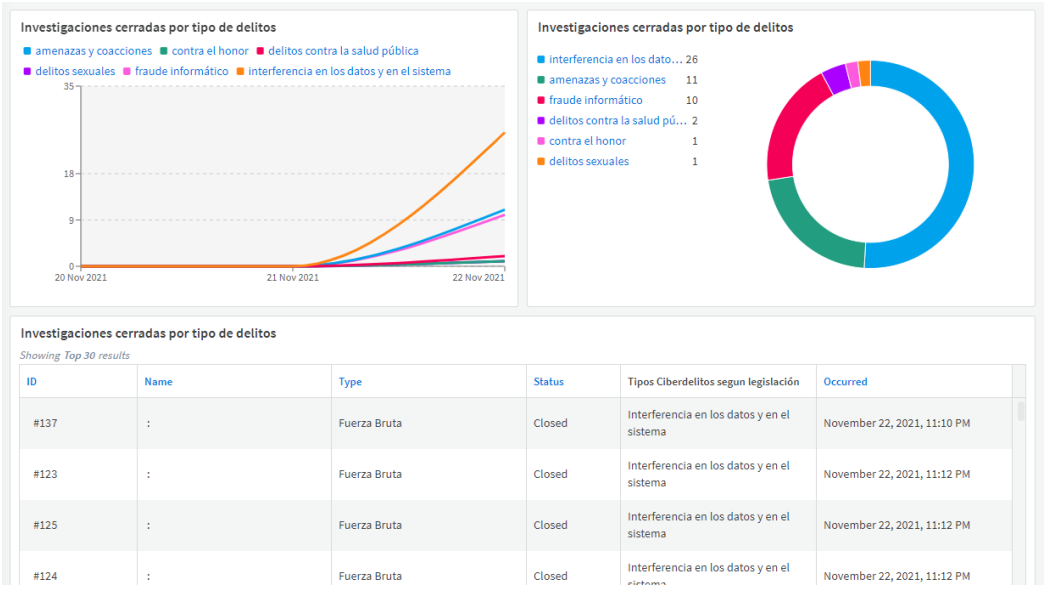


Ilustración 15 - Ejemplo cuadro de mandos tipos de ciberdelitos

3.4. Arquitectura

A continuación, se presenta el diagrama de arquitectura con los diferentes servicios y servidores que han sido utilizados para desarrollar y ejecutar la prueba de concepto.

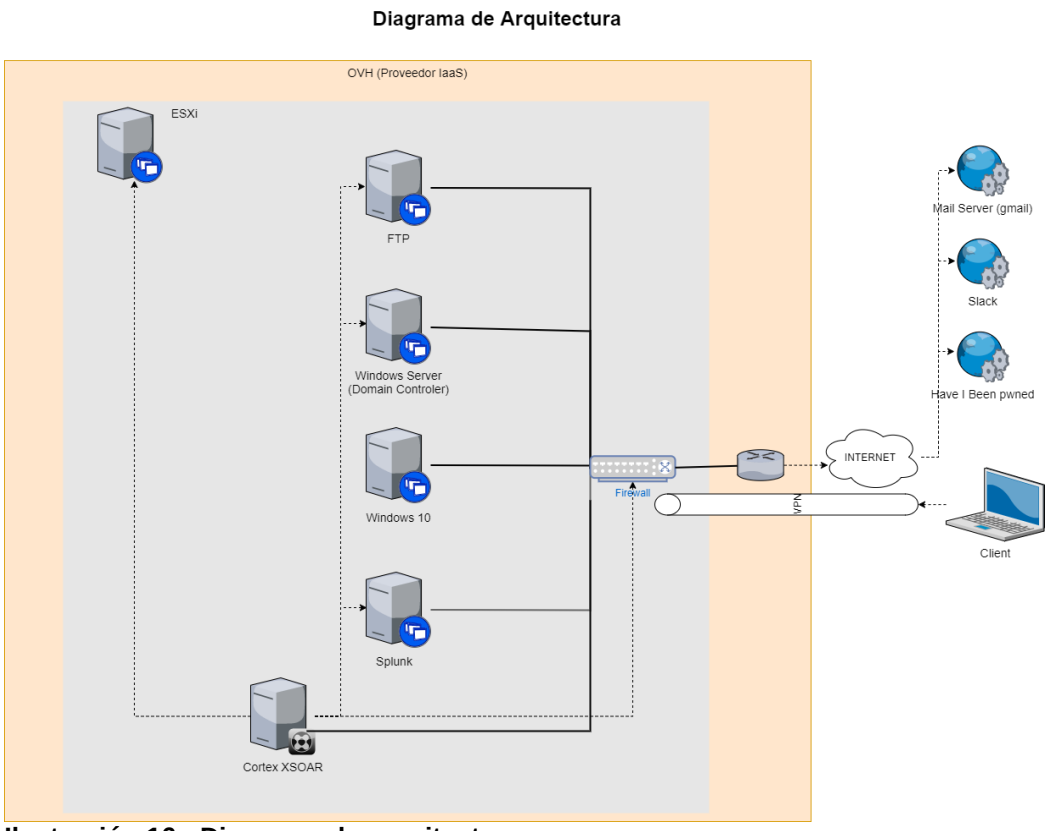


Ilustración 16 - Diagrama de arquitectura

La arquitectura mostrada en el diagrama anterior se encuentra en un entorno 100% virtualizado montado sobre un ESX a excepción del router y las herramientas de terceros ubicadas en internet.

Todas las herramientas a continuación descritas han sido montadas con licencias de estudiantes o bien licencias de evaluación cedidas por los diferentes fabricantes u organizaciones a excepción del servicio Have i been pwned.

El entorno se compone de:

- SOAR Cortex XSOAR versión 6.2
- Servidor FTP Windows IIS
- SIEM Splunk 8.2
- OS Windows 10
- Hypervisor vsphere 6.2
- Firewall Palo Alto Networks v9

Como componentes externos a nuestros sistemas contamos con:

- Servido de Mail Gmail
- Servidor de mensajería SLACK
- Servidor de envío SMS Twillo
- Leaks Have i been pwned

El servidor FTP y el servidor de dominio envían todos los eventos de seguridad al SIEM Splunk.

El firewall envía todas las peticiones hacia IP categorizadas como maliciosas directamente al SOAR por syslog. (El objetivo es buscar una alternativa viable al uso del SIEM como ejercicio durante la POC).

3.5. Integraciones

A continuación, se presenta una tabla con las integraciones configuradas en la herramienta SOAR, tipo de herramienta y una breve descripción.

Integración	Tipo de integración	Descripción
Splunk	Analítica y SIEM	Permite la realización de consultas a Splunk y lectura de alertas.
Syslog	Analítica y SIEM	Permite la recepción de mensajes de syslog para abrir investigaciones.
Active Directory	Enriquecimiento de datos e inteligencia sobre amenazas	Realiza consultas en el Active Directory, permitiendo acceder y administrar objetos como usuarios, contactos y computadoras.
Have I Been Pwned	Enriquecimiento de datos e inteligencia sobre amenazas	Servicio para comprobar si las direcciones de correo electrónico, los dominios o los nombres de usuario se vieron comprometidos y filtrados
VmWare	Servicios IT	Administra vCenter permitiendo administrar máquinas virtuales y hosts ESX de forma centralizada.
Mail Listener	Mensajería	Lectura de emails por IMAP
Mail Sender	Mensajería	Envía correos electrónicos
Slack	Mensajería	Envía notificaciones a canales o usuarios de Slack.
Twillo	Mensajería	Envía SMS
AnsibleVMware	Servicios IT	Administra vCenter permitiendo administrar máquinas virtuales y hosts ESX de forma centralizada.

Tabla 37 - Integraciones utilizadas en POC

4. Propuesta de valor

Para realizar la propuesta de valor se ha utilizado la metodologia canvas, completando el siguiente lienzo donde se ha modificado la primera cuadricula respecto a la propuesta mas extendidad en la red y donde se situan a los socios o partners clave, por los problemas.

El lienzo canvas utilizado para generar la propuesta de valor resultante es el siguiente:

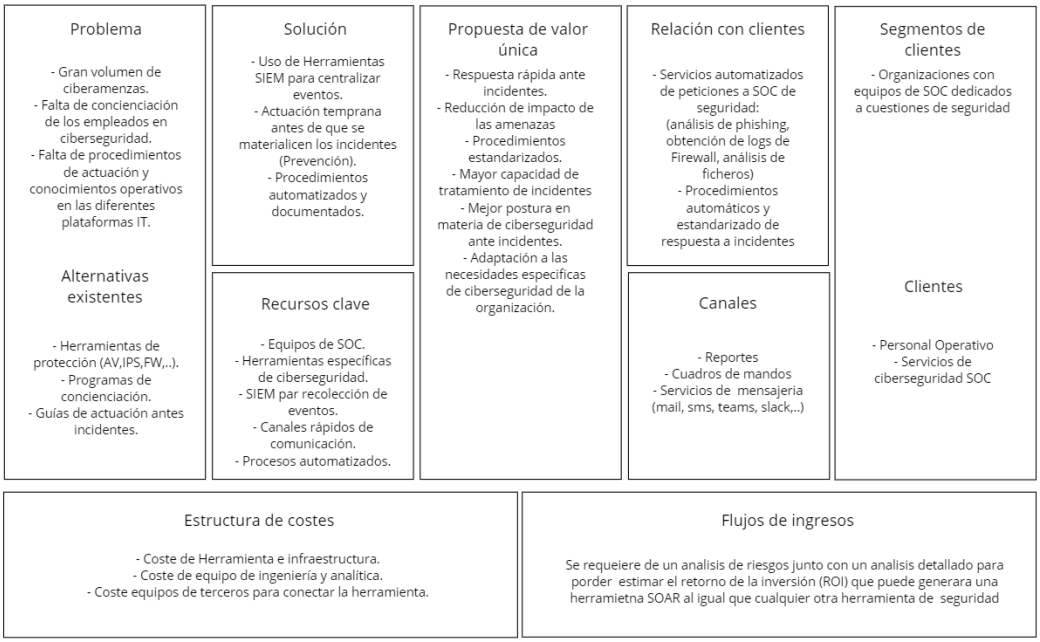


Ilustración 17 - Lienzo canvas propuesta de valor

Propuesta de valor del uso de herramientas SOAR en la organización

- Respuesta rápida ante incidentes.
- Reducción de impacto de las amenazas
- Procedimientos estandarizados.
- Mayor capacidad de tratamiento de incidentes.
- Mejor postura en materia de ciberseguridad ante incidentes.
- Adaptación a las necesidades especificas de ciberseguridad de la organización.

5. Análisis de los objetivos

Como parte del proyecto a continuación, se asignará una puntuación a los diferentes objetivos marcados al inicio en base a la siguiente tabla de puntuación para poder determinar si se han cumplido.

Puntuación	Resultado
1	Muy por debajo de lo esperado.
2	Por debajo de lo esperado.
3	Resultado esperado.
4	Por encima de lo esperado.
5	Muy por encima de lo esperado.

Tabla 38 - Métrica evaluación objetivos

Objetivo general:

Objetivo	**Generar una propuesta de valor que permita mejorar la postura de seguridad de las organizaciones mediante el uso de herramientas SOAR**
Puntuación	Por encima de lo esperado.
Justificación	El uso de las herramientas SOAR son la mejor solución hasta la fecha para mejorar el tratamiento de incidentes ayudando a reducir el posible impacto de las amenazas de forma metódica ágil y adaptándose a las diferentes realizades tecnológicas de las organizaciones. Como punto negativo no es posible calcular un retorno de la inversión de forma generalista al igual que sucede con el resto de las herramientas que tienen como objetivo la prevención y mitigación.

Tabla 39 - Evaluación objetivo general

Objetivos específicos:

Objetivo	**Estudio de los diferentes tipos de ciberamenzas potenciales que sufren las diferentes organizaciones y derivan en incidente.**
Puntuación	Por debajo de lo esperado.
Justificación	No se ha conseguido acceso a una fuente de información de organizaciones públicas con un nivel de detalle y clasificaciones adecuados que permitan determinar el impacto de las diferentes amenazas. Las fuentes públicas consultadas han evidenciado que el tipo de información buscada no quiere ser divulgada por las organizaciones y que existen diferentes hándicaps en lo que refiere a su obtención y clasificación.

Tabla 40 - Evaluación objetivo específico 1

Objetivo	**Análisis y definición de criterios que permita determinar estadísticamente que amenazas son más relevantes.**
Puntuación	Resultado esperado.
Justificación	Desde el inicio del proyecto, se conocía que cubrir este objetivo dependería del acceso y la calidad de la información obtenida durante la investigación. Aunque estadísticamente ha sido posible extraer conclusiones en base a un sistema de clasificación. Los datos obtenidos no han permitido determinar

	el impacto real de los diferentes tipos de amenazas investigadas.

Tabla 41 - Evaluación objetivo específico 2

Objetivo	**Diseño y propuesta de remediación de amenazas potenciales mediante el uso de herramientas SOAR.**
Puntuación	Resultado esperado.
Justificación	Los resultados han sido satisfactorios, no obstante, el proceso de cómo se debería tratar un incidente, en lo que refiere al diseño no aporta ninguna innovación a la forma en cómo se aborda el problema. La única forma de mejorar los resultados esperados sería adelantarnos a la alerta o el evento que dispara los casos de uso por ejemplo añadiendo algoritmos predictivos o bien añadiendo técnicas de machine learning a la toma de decisiones dentro de los flujos definidos.

Tabla 42 - Evaluación objetivo específico 3

Objetivo	**Prueba de concepto en un entorno de laboratorio.**
Puntuación	Muy por encima de lo esperado.
Justificación	Se han cubierto tres casos de uso y diferentes tipos de disparadores. Esto sirve de muestra conforme las soluciones SOAR son flexibles y que no es estrictamente necesario el uso de tecnologías SIEM como disparador de los diferentes flujos.

Tabla 43 - Evaluación objetivo específico 4

6. Conclusiones

Como consecuencia del proyecto se han extraído diversas conclusiones que puede derivar en mejoras, nuevas líneas de actuación, incluso en como deberían ser los nuevos perfiles necesarios para trabajar en los equipos de SOC.

En primer lugar, podemos afirmar que el objetivo global se ha cumplido. Tenemos una propuesta de valor para el uso de herramientas SOAR. Desafortunadamente no ha sido posible incluir el cálculo del retorno de la inversión como parte del proceso de creación de la propuesta de valor. Calcular el ROI es complejo y no se puede realizar de forma generalista, ya que podría dar lugar a error. Entre otros motivos, el principal, es que la postura de seguridad frente a los diferentes tipos de amenazas se ha de mejorar día a día, ya que las amenazas también lo hacen. Ya sea mejorando la monitorización, gestión de incidentes, metodologías de actuación, incorporación de nuevas soluciones, ... Si consideramos que no existe la seguridad absoluta se requerirá de un proceso de mejora continua. Adicionalmente, evaluar el coste potencial de aquellas brechas de seguridad que debido a la actuación de la solución no se han materializado complica la tarea de calcular el retorno de la inversión.

En lo que refiere a los objetivos asociados a la fase de investigación, podemos afirmar que no existe un conjunto de datos lo suficientemente detallado ni completo que permita determinar que tipología de incidentes son los que causan un mayor impacto. De la misma forma, al no contar con el detalle de las amenazas no es posible definir un criterio que nos permita establecer el impacto aproximado de los diferentes tipos de amenazas.

Algunos de los problemas que han surgido durante la investigación, han sido la falta de información con detalle. Solo se han podido obtener datos agregados de las diferentes administraciones. La experiencia obtenida durante la recolección de información en el proyecto de las diferentes fuentes me ha hecho llegar a las siguientes hipótesis.

- Las organizaciones públicas o infraestructuras críticas no están notificando todas las amenazas detectadas.
- Las organizaciones privadas no tienden a compartir su información sobre amenazas detectadas.
- No existe un sistema de clasificación consistente que permita realizar analítica ni mejoras.
- Las capacidades de detección están intrínsicamente relacionadas con las plataformas de detección y protección.

Por lo tanto, dentro de las diferentes líneas de mejora que se puede derivar del apartado de investigación; la principal sería la de establecer un modelo de clasificación y registro detallado de incidentes que permita compartir de forma anónima información sobre las amenazas detectadas y resultados de la investigación, así como de las acciones tomadas. Un

conjunto de datos lo suficientemente detallado y bien estructurado abriría las puertas a trabajos analíticos más complejos.

Respecto a los objetivos de las fases de diseño de casos de uso y POC se puede afirmar que han sido logrados. En primer lugar, ha sido posible plantear hasta tres casos de uso diferentes para dar respuesta a diferentes tipos de incidentes de forma genérica. En segundo lugar, la prueba de concepto realizada a abordado la implementación completa de los tres diseños propuestos más un sistema de clasificación personalizado.

Podemos concluir que el uso de herramientas SOAR es beneficioso para mejorar el tratamiento de las diferentes amenazas y que estas redundan en una mayor productividad frente a un modelo sin automatización. La estandarización de procedimientos permitirá a los diferentes analistas de un SOC operar de forma metódica y ordenada, dejando registro detallado de cualquier acción o toma de decisión realizada de forma manual y automática. La reducción de los tiempos de respuesta es evidente en procesos que operan 24/7 de forma automática. No obstante, existe el riego de que una dependencia muy alta de acciones o decisiones manuales que requieran de los analistas, resulte en tiempos tratamiento de amenazas elevados. Esto se evitaría mediante un alto nivel de automatización de los procesos y por lo tanto con la definición de casos de uso con grandes niveles de complejidad que podrían requerir desarrollos a medida.

De la fase de diseño y POC propondría como línea de mejora del proyecto la creación de automatismos que permitan decidir qué acciones condicionales realizar a partir del tratamiento de los diferentes tipos de amenazas analizados en el pasado. Es decir, en ocasiones se solicita a los analistas que tomen una decisión sobre qué acción tomar. Se trataría de ampliar la POC con un algoritmo predictivo que a partir de los datos del incidente en curso y las decisiones tomadas en incidentes similares anteriores, se puedan determinar las acciones a tomar más habituales, reduciendo el tiempo de respuesta a incidentes.

Como aspectos a considerar, podemos determinar que este tipo de herramientas, aunque faciliten gran cantidad de playbooks, integraciones, automatismos ya preconfigurados, siguen requiriendo de equipo formado para gestionar la solución y de equipo analista con conocimientos de ciberseguridad. Por lo tanto, el uso de herramientas SOAR debería ir asociado a equipos de trabajo multidisciplinares, donde al menos se contemplen los skills de desarrollador y analista de ciberseguridad.

Finalmente, en lo que respecta a la planificación del proyecto se ha respetado con algunas modificaciones. Las modificaciones realizadas han sido calculadas y promovidas por la motivación de tratar de realizar varios casos de uso funcionales con diferentes vectores de activación y sin afectación de los hitos marcados.

7. Glosario y acrónimos

Definición de los términos y acrónimos más relevantes utilizados dentro de la Memoria.

Lista de acrónimos:

ACN	Activos Críticos de Negocio
AD	del inglés "Active Directory" Directorio activo
C&C	del inglés "Command and Control" Mando y control
C2	del inglés "Command and Control" Mando y control
CERT	del inglés "Computer Emergency Response Team" Equipo de Respuesta ante Emergencias Informáticas
CVE	del inglés "Common Vulnerabilities and Exposures" Vulnerabilidades y exposiciones comunes
FTP	del inglés "File Transfer Protocol" Protocolo de transferencia de archivos
GDPR	del inglés "General Data Protection Regulations" Reglamento General de Protección de Datos
IDE	del inglés "Integrated Development Environmen" Entorno de desarrollo integrado
IDS	del inglés "Intrusion Detection System" Sistema de detección de intrusos
IoT	del inglés "Internet Of Things" Internet de las cosas
IPS	del inglés "Intrusion Prevention System" Sistema de prevención de intrusos
IT	del inglés "Internet Of Things" Internet de las cosas
MISP	del inglés "Malware Information Sharing Platforms" Plataforma para compartir información sobre ciberamenazas
NAC	del inglés "Network Access Control" Control de acceso a red
NIST	del inglés "National Institute of Standards and Technology" Instituto Nacional de Estándares y Tecnología
OS	del inglés "Operating system" Sistema operativo
POC	del inglés "proof of concept" Prueba de concepto
ROI	del inglés "Return On Investment" Retorno de la inversión
SIEM	del inglés "Security Information and Event Management" Seguridad de la información y gestión de eventos
SOAR	del inglés "Security Orchestration Automation and Response" Orquestación de Seguridad, Automatización y Respuesta
SOC	del inglés "Security Operation Center" Centro de operaciones de seguridad

8. Bibliografía

Lista numerada de las referencias bibliográficas utilizadas dentro de la memoria.

Betancourt, D. (28 de 12 de 2021). *Sitio web: ingenioempresa*. Obtenido de https://www.ingenioempresa.com/lienzo-de-propuesta-de-valor/

Centro Criptológico Nacional. (28 de 12 de 2021). *Documento de sitio web: Informe ciberamenazas tendencias 2019.* Obtenido de https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3776-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-edicion-2019-1/file.html

Centro Criptológico Nacional. (28 de 12 de 2021). *Documento de sitio web: Informe ciberamenazas tendencias 2020.* Obtenido de https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/5377-ccn-cert-ia-13-20-ciberamenazas-y-tendencias-edicion-2020/file.htm

Centro Criptologico Nacional. (28 de 12 de 2021). *Sitio web:CCN-CERT*. Obtenido de https://www.ccn-cert.cni.es/

Check Point Software Technologies LTD. (28 de 12 de 2021). *Documento de sitio web: Cybersecurity Report 2021.* Obtenido de https://pages.checkpoint.com/cyber-security-report-2021.html

Crowdstrike. (28 de 12 de 2021). *Documento de sitio web: Crowdstrike services cyber front lines report.* Obtenido de https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2020CrowdStrikeServicesCyberFrontLines.pdf

Detectionlab. (28 de 12 de 2021). *Sitio web: detectionlab*. Obtenido de https://www.detectionlab.network

EINSA. (28 de 12 de 2021). *European Union Agency for cybersecurity*. Obtenido de https://www.enisa.europa.eu/

Instituto nacional de ciberseguridad. (28 de 12 de 2021). *Sitio web: INCIBE*. Obtenido de https://www.incibe.es/

Metricool. (28 de 12 de 2021). *Sitio web: Metricool*. Obtenido de https://metricool.com/es/propuesta-de-valor/

Ministerio del Interior de España. (28 de 12 de 2021). *Documento de sitio web: Estudio sobre la cibercriminalidad en España en 2019.* Obtenido de http://www.interior.gob.es/documents/10180/9814700/Estudio+sobre+la+Cibercriminalidad+en+Espa%C3%B1a+2019.pdf/24bd3afb-5a8e-4767-9126-c6c3c256982b)

Noticias Jurídicas. (28 de 12 de 2021). *Sitio web: Noticias Juridicas*. Obtenido de https://noticias.juridicas.com/base_datos/Penal/lo10-1995.html

Oberlo. (28 de 12 de 2021). *Sitio web: Oberlo*. Obtenido de https://www.oberlo.es/blog/propuesta-de-valor

Observatorio español de delitos informáticos. (28 de 12 de 2021). *OEDI*. Obtenido de https://oedi.es/

Observatorio Nacional de Tecnología y Sociedad. (28 de 12 de 2021). *Sitio web: ONTSI.data*. Obtenido de https://www.ontsi.es

Palo Alto Networks. (28 de 12 de 2021). *Documentode sitio web: XSOAR State of SOAR report 2020.* Obtenido de https://www.paloaltonetworks.com/cortex/xsoar-state-of-soar-report-2020

Palo Alto Networks. (28 de 12 de 2021). *Sitio web: Cortex XSOAR*. Obtenido de https://xsoar.pan.dev/

Palo Alto Networks. (28 de 12 de 2021). *Sitio web: Palo Alto Networks | TechDocs Home*. Obtenido de https://docs.paloaltonetworks.com

SANS. (28 de 12 de 2021). *Sitio web: SANS*. Obtenido de https://www.sans.org

Secretaría de estado de digitalización e inteligencia artificial. (28 de 12 de 2021). *Sitio web: ONTSI Data*. Obtenido de https://servicesqap.red.es/single/?appid=c39c3c09-4e12-4485-b662-ee2673c46ec2&sheet=b7571d1f-4979-484d-aa73-02ee06fe749f

Splunk. (28 de 12 de 2021). *Documento de sitio web: IT Security predictions.* Obtenido de https://datatoeverything.id/asset/2020-splunk-tl-splunk-predictions-2020-Security-EN.pdf

Splunk. (28 de 12 de 2021). *Documento de sitio web: State of security 2021.* Obtenido de https://www.splunk.com/en_us/pdfs/resources/e-book/splunk-state-of-security-2021.pdf

Verizon. (28 de 12 de 2021). *Documento de sitio web: 2021 Data breach investigations report.* Obtenido de https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf

Yun, T. (28 de 12 de 2021). *Sitio web: Modelo Canvas*. Obtenido de https://modelocanvas.net/propuesta-de-valor/

9. Anexos

Listado de carpetas y documentos realizados como material de apoyo que complementan y amplían el trabajo realizado:

Carpeta: 1 - Planificaciones
Descripción: Planificación global del proyecto inicial y final.
Contenido:
- Fichero planificación inicial en formato PDF
- Fichero planificación final en formato PDF

Carpeta: 2 - Diagramas de arquitectura
Descripción: Mapa completo de los equipos y servicios utilizados para la realización de la POC.
Contenido:
- Fichero en formato VSD
- Fichero en formato PNG

Carpeta: 3 - Diagramas de casos de uso
Descripción: Imágenes de los diagramas de los casos de uso diseñados con alto nivel de resolución.
Contenido:
- Imagen playbook acceso no autorizado (Fuerza bruta) - core
- Imagen playbook malware (C2) - core
- Imagen playbook robo de credenciales (Data Leak) - core
- Imagen playbook robo de credenciales (Data Leak) - email
- Imagen playbook robo de credenciales (Data Leak) - job

Carpeta: 4 - Documentación técnica
Descripción: Documento con las especificaciones básicas de todos los elementos y descripciones utilizados en el orquestador.
Contenido:
- Fichero en formato PDF

Carpeta: 5 - Content pack
Descripción: Paquete instalable con los desarrollos y definición de objetos realizados en Cortex XSOAR.
Contenido:
- Ficheros de playbooks en formato YML
- Ficheros de tipos de incidentes en formato JSON
- Ficheros de campos de incidentes en formato JSON
- Ficheros de clasificadores en formato JSON
- Ficheros de automatismos en formato YML

Carpeta: 6 - Propuesta de valor
Descripción: Documento con el diagrama canvas utilizado para realizar la propuesta de valor con alto nivel de resolución.
Contenido:
- Fichero en formato PDF