Desarrollo e implementación de un SOC en una organización

Juan Peña Juarez
Máster de Seguridad de las Tecnologías de la Información y las Comunicaciones (UOC, URV, UAB)
Seguridad empresarial

Director del TFM
Daniel Brande Hernandez

Profesor responsable de la asignatura
Victor Garcia Font

Fecha Entrega
1 de Junio de 2021

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Desarrollo e implementación de un SOC en una organización*
Nombre del autor:	*Juan Peña Juarez*
Nombre del consultor/a:	Daniel Brande Hernandez
Nombre del PRA:	Victor Garcia Font
Fecha de entrega (mm/aaaa):	06/2021
Titulación:	Máster de Seguridad de las Tecnologías de la Información y las Comunicaciones
Área del Trabajo Final:	*Trabajo final del master*
Idioma del trabajo:	*Castellano*
Palabras clave	*SOC, SIEM,IDS*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

La finalidad de este trabajo es crear un marco de trabajo para la implementación de un SOC en una organización. Debido a la pandemia las organizaciones han cambiado su organización y se han visto obligadas a digitalizarse de golpe, con este trabajo se pretende ayudar a implementar un SOC con el fin de proteger al máximo sus activos. Por ello se han ido estudiando diferentes marcos de trabajo existentes y normativas para ir definiendo las partes de un SOC y los criterios para su implementación, pero en paralelo a la parte teórica se ha ido realizando una parte práctica, en la que siguiendo los pasos de la guía que iba confección, iba implementando un SOC en la organización para la que trabajo, de forma que al final el trabajo tuviera una guía de implementación y un SOC real implementado en un entorno real.

Finalmente, las conclusiones obtenidas son satisfactorias, se ha elaborado una guía para la implementación de un SOC que cubre todas las necesidades que una organización pueda tener, además de una implementación practica de un SOC que pueden tomar como referencia para realizar la suya propia.

Abstract (in English, 250 words or less):

The purpose of this paper is to create a framework for the implementation of a SOC in an organisation. Due to the pandemic, organisations have changed their organisation and have been forced to go digital all at once. The aim of this work is to help implement a SOC in order to protect their assets as much as possible. For this reason, different existing frameworks and regulations have been studied in order to define the parts of a SOC and the criteria for its implementation, but in parallel to the theoretical part, a practical part has been carried out, in which, following the steps of the guide that was being prepared, a SOC was implemented in the organisation for which I work, so that at the end the work had an implementation guide and a real SOC implemented in a real environment.

Finally, the conclusions obtained are satisfactory, a guide has been produced for the implementation of a SOC that covers all the needs that an organisation may have, as well as a practical implementation of a SOC that can be used as a reference for their own.

Índice

Lista de figuras

Lista de tablas

1. Introducción

1.1 Contexto y justificación del Trabajo

Este proyecto de fin de master nace de la problemática surgida en materia de seguridad informática, que la pandemia de covid-19 ha provocado en muchas organizaciones. Debido a que por motivos de salud han tenido que realizar cambios en su organización, pasando muchos de sus empleados a teletrabajar desde casa, pero esta adaptación ha sido forzada y con urgencias, no estaban preparadas para este cambio, esto ha ocasionado que se encuentren mucho más expuestas a ciberataques ya que se ha aumentado la superficie de exposición y no todas han podido securizar correctamente sus nuevas estructuras, no han tenido el tiempo suficiente para planificarlo, ni para cambiar sus protocolos de seguridad.

El principal objetivo de este TFM es la de crear un marco de trabajo para implementar un SOC[1] (centro de operaciones de seguridad) en una organización. Un SOC, según las películas, es esa sala grande llena de pantallas donde en plena noche saltan todas las alarmas porque hay un intruso en la red. El SOC debe ayudar a monitorizar la actividad de la red, detectar posibles amenazas, gestionar los incidentes de seguridad y realizar un análisis forense de los ataques recibidos para mejorar las medidas de seguridad. Este marco se irá elaborando mientras se va realizando una implementación real en la empresa para la cual trabajo. Es por ello que en este TFM se trabajará en dos áreas, por un lado, la parte teoría donde se irá confeccionando el marco de trabajo, definiendo los pasos que se han de seguir para su correcta implementación y a su vez en la parte práctica con la implementación real de un SOC siguiendo ese marco de trabajo.

En la parte teórica se realizará un trabajo de investigación sobre los fundamentos teóricos de un SOC, que elementos lo componen, las fases necesarias para su implementación, que recursos necesita, el personal necesario y como debe encajar dentro del organigrama de IT actual de la empresa. Con esa información se irá elaborando un marco de trabajo que ayude y guíe a una organización a diseñar e implementar un SOC acorde a sus necesidades y recursos de los que dispone, pero que aseguré un nivel de protección suficiente.

En la parte práctica se irá siguiendo paso a paso el marco de trabajo que se vaya elaborando en la parte teórica, para realizar la implementación real en una organización, se realizaran un estudio para encontrar un desarrollo open source de cada uno de los elementos del SOC, que aseguren una implementación de calidad. Se instalarán las balizas, los escáneres de vulnerabilidades, los IDS/IPS[2], los analizadores de protocolo, el SIEM, etc. Y se realizaran todas las pruebas necesarias para comprobar su correcto funcionamiento además de entrenar al equipo para el análisis y respuesta frente a amenazas.

[1] https://es.wikipedia.org/wiki/Centro_de_operaciones_de_seguridad
[2] https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

La implementación de la parte práctica se realizará en la empresa donde actualmente trabajo, es una operadora de telefonía móvil para equipos de emergencia e IoT[3], donde se comercializan líneas telefónicas, se fabrican dispositivos de emergencia y conectividad para conectar los equipos a internet, monitorizarlos y dar servicios de valor añadido como la telegestión o telemantenimiento. Dispone de un departamento de i+d+i donde se diseñan estos equipos, un departamento de fabricación donde se ensamblan y prueban, el departamento comercial y el departamento de administración, en total más de 20 empleados, de los cuales hay que se encuentran teletrabajando permanentemente en estos momentos y otros que realizan un trabajo hibrido entre el teletrabajo y el presencial. La empresa tiene servidores en la nueve para dar sus servicios además de una nueva línea comercial de servicios de IOT, tanto para el sector de emergencia como para las comunidades de propietarios. En los últimos años gracias a la creación del departamento de i+d+i y poder ofrecer productos propios diferenciadores, la empresa ha sufrido un rápido crecimiento, ha pasado de ser una empresa familiar de pocos empleados a los actuales en pocos años, esto ha hecho que a pesar de invertir en mejoras en materia de seguridad informática, no tenga sus infraestructuras suficientemente preparadas para los nuevos cambios, de ahí que sea un entorno propicio para la realización de este trabajo de fin de master, ya que es un buen ejemplo de los retos a los que se enfrenta una organización en estos días y cuál sería el camino a seguir para mejorar.

La empresa para que trabajo me ha brindado su total apoyo, pero prefiere que no divulgue su nombre, ya que se va a desvelar en este trabajo de fin de master información sobre su red interna y prefiere que no se relacione.

1.2 Objetivos del Trabajo

Este trabajo de fin de master tiene los siguientes objetivos por área:

1.2.1 Objetivos de la parte teórica.

- Investigar sobre las principales normativas y guías de buenas prácticas relativas a un SOC, ISO27001, el informe SOC2, ENISA, el VSOC del CCN o él MITRE, para asegurar que se vean incluidas en el marco de trabajo a presentar.
- Investigar sobre las funciones y estructura de un SOC.
- Investigar sobre las diferentes partes que lo componen.
- Investigar el proceso de integración de un SOC en la estructura existente de una organización.
- Definir un marco de trabajo para la integración de un SOC.
- Documentar todo el proceso.

[3] https://es.wikipedia.org/wiki/Internet_de_las_cosas

1.2.2 Objetivo de la parte práctica:

- Instalación y configuración de un servidor en la red donde se realizará el control de la red.
- Aprender a instalar y configurar las balizas y analizadores de red que aportaran la información al SOC.
- Aprender a instalar y configurar un SIEM en el cual se gestionará toda la información recibida para ser analizada por el personal del SOC.
- Aprender a configurar y crear reglas para la detección de amenazas en el sistema.
- Formar al personal del SOC en sus tareas diarias.
- Poner en marcha el SOC y la realización de pruebas para la validación y calibración de los sistemas.

1.2.3 Objetivos principales

Principalmente como ya se ha mencionado los objetivos del trabajo de fin de master son dos, crear un marco de trabajo para la implementación de un SOC en una organización y la implementación real de un SOC en la empresa para la que trabajo. Eso conlleva que al final del proyecto se han de haber cumplido los siguientes objetivos:

- La creación de una guía para que los profesionales de it a implementen un SOC en su empresa.
- Un SOC operativo en una organización implementado siguiendo la guía anteriormente creada.
- Personal en una organización formado para la responder a las posibles amenazas.
- Mejora de la ciberseguridad de una organización y un protocolo de respuesta a incidentes de seguridad.

1.3 Enfoque y método seguido

Este trabajo de fin de master está dividido en dos partes claras y definidas, la parte teórica, que consisten en investigación y creación del marco de trabajo, y una parte práctica donde se implementara un SOC en una organización real.

En principio, para la realización del trabajo se podría utilizar una metodología en cascada, donde primero se realizara todo el trabajo teórico, en el cual se definirán todos los requisitos y la forma de trabajo que se debe llevar a cabo en la parte práctica, y una vez completados se realizaría la implementación del SOC según se ha definido en la parte teórica, pero esta metodología presenta el inconveniente que si surgiera algún problema durante la implementación y esto obligase a cambiar la metodología, podría ocasionar que todo el trabajo realizado desde ese punto se tuviera que repetir con la consiguiente pérdida de tiempo y de recursos, por ello se utilizará una metodología agile.

En la metodología agile en cada fase del trabajo teórico se llevará a cabo la parte práctica, de forma que se compruebe que el marco de trabajo teórico es correcto, y si no fuera así se volvería a realizar una iteración sobre esa fase

hasta llegar a un resultado correcto. Esto asegura que cada vez que se complete una fase ya se obtendrá una parte de la implementación del SOC funcional, y al terminar el trabajo teórico también se tendrá completado el trabajo practico. Este tipo de metodología también encaja mejor con la planificación de entregas continuas de la UOC, de forma que en cada entrega ya se entregará una parte completa del proyecto que se podrá evaluar.

Pero como hilo conductor de proyecto en la parte práctica comenzará analizando el estado del arte, para conocer actualmente que existe, para ayudar a definir la estructura de trabajo, cuáles son los principales servicios que tiene que ofrecer un SOC, en que tecnologías está basado, y cuáles son las operaciones que realiza.

En la parte práctica se estudiará la estructura actual de la organización, para ver qué elementos actuales que ya tenga se pueden utilizar, y ver cuales necesita para cubrir los servicios necesarios, que estructuras hay que proteger y monitorizar, cuáles serían las tecnologías idóneas para hacerlo e implementarlas.

1.4 Planificación del Trabajo

1. Planificación
2. Introducción a los SOC
    a. Que es un SOC.
    b. Estructura de un SOC
3. Estudio de la red actual de la organización
    a. Estructura de la red.
        i. Elementos ya existentes utilizables en el SOC
    b. Definición de los activos a proteger.
        i. Definición de sistemas críticos
        ii. Definición de sistemas necesarios
        iii. Definición de sistemas con información sensible
4. Detección de los activos vulnerables
    a. Análisis de vulnerabilidades.
5. Identificación de las amenazas
    a. Detección de intrusos (IDS/IPS)
    b. Agentes en los hosts
6. Brechas de seguridad
    a. Captura de paquetes TCP/IP
    b. Análisis de protocolos
7. Análisis de los datos.
    a. SIEM
8. Estructura del personal del soc.
    a. Personal de primer nivel
    b. Personal de segundo nivel
    c. Personal de tercer nivel.
9. Informe del TFM
    a. Memoria Final del TFM
    b. Presentación.
    c. Defensa.

FASE		DETALLES	T1												T2											
			ENE			FEB				MAR					ABR				MAY					JUN			
	SEMANA DEL PROYECTO:			1	8	15	22	1	8	15	22	29	5	12	19	26	3	10	17	24	31	7	14	21	28
1	Planificación	- Objetivos y planificación del proyecto																								
2	Introducción a los SOCS	- Que es un SOC - Estructura de un SOC																								
3	Estudio de la red actual de la organización	- Estructura de la red - Elementos ya existentes utilizables en el SOC																								
4	Definición de los activos a proteger	- Definición de sistemas críticos - Definición de sistemas necesarios - Definición de sistemas con información sensible																								
5	Detección de los activos vulnerables	- Análisis de vulnerabilidades																								
6	Identificación de las amenazas	- Detección de intrusos (IDS/IPS) - Agentes en los hosts																								
7	Detección de las brechas de seguridad	- Captura de paquetes TCP/IP - Análisis de protocolos																								
8	Análisis de los datos	- SIEM																								
9	Estructura del personal del soc	- Análisis final - Lista de deficiencias del proyecto - Informe																								
10	Informe del TFM	- Memoria Final del TFM -Presentación - Defensa																								

1.5 Estado del arte

Trend Micro incorporated ha anunciado en su informe 'Un estado de cambio constante: Informe anual de ciberseguridad de Trend Micro 2020' que el año pasado se produjeron 62.600 millones de ciberamenazas, aumentando un 20%, también dice que los hogares sufrieron un 210% más de ataques, hasta casi 2.900 millones, un 15,5% del total de hogares atacados. El 73% de los ataques a las redes domésticas intentaban obtener el control del router o de algún dispositivo inteligente a través de ataques de fuerza bruta. Ya que debido al teletrabajo un gran número de personas trabajaban desde casa se volvió un punto de acceso a las infraestructuras de las empresas más sencillo y vulnerable.

Como comentaba en el primer apartado las empresas han visto aumentada su superficie de exposición frente a los ataques, antes tenían que proteger únicamente sus infraestructuras, desde el router de la oficina hacía dentro, pero ahora tienen que proteger sus infraestructuras y las de sus empleados teletrabajando, ya que al conectarse por vpn a la empresa se convierten en una parte de la red de está, pero mucho más expuesta al no disponer en casa de elementos de securización. Aparte se han publicado muchos más servicios en la nube, para cubrir la necesidad de seguir dando sus servicios que antes se podían dar de forma física, ahora se tienen que hacer online, como el aumento de la venta online, muchas empresas han abierto tiendas en internet durante la pandemia y las que ya las tenían han visto aumentado su volumen de trabajo. Las clases y cursos online, las reuniones por videoconferencia etc. Todo esto ha aumentado el número de posibles objetivos para los ciberdelincuentes, con las redes lanzadas sobre internet a la búsqueda de un servidor mal configurado, un servicio con las credenciales por defecto o una vulnerabilidad no parcheada.

1.5.1 Definición de un SOC

En el apartado 2 de este trabajo se ampliará la información, pero de forma resumida, un SOC o Centro Operaciones de Seguridad (Security Operations Center, en inglés, de ahí sus siglas) es el lugar donde se centraliza el análisis de la actividad de una red informática, para detectar actividades sospechosas que puedan indicar que se está produciendo un incidente de seguridad. En el SOC trabaja un equipo humano especializado, que mediante el uso de equipos y software específico es el responsable de la seguridad informática de la organización.

1.5.2 Tipos de SOC según su organización

Según su organización se podrían definir tres tipos de SOC:

- **Distribuido**, bien porque la organización es muy grande y centraliza en una única instalación la vigilancia y monitorización de todas sus sedes, o bien por justo lo contrario, que sea muy pequeña para disponer de un SOC propio y contrate los servicios de una empresa especializada.
- **Mixto**, la organización tiene un SOC propio, pero no dispone de los analistas de todos los niveles necesarios, de forma que contrata los

servicios de análisis de más alto nivel. O tiene los recursos para un SOC 8x5 y subcontrata el resto de servicios a un SOC 24x7.
- **Físico**, la empresa dispone de suficientes recursos para disponer de todo el personal necesario y del equipamiento para llevar a cabo una monitorización y respuesta de incidentes 24x7.

1.5.3 Personal del SOC

El personal de un SOC se puede dividir en tres niveles según su grado de especialización y formación.

- **Nivel 1**. Son los analistas que monitorizan la actividad buscando anomalías y se ocupan de dar la alerta en caso de ocurrir un incidente.
- **Nivel 2**. Son los analistas encargados de realizar la auditoría del incidente, establecer que servicios y que datos se han visto comprometidos y de recomendar una respuesta.
- **Nivel 3**. Son los analistas más cualificados que se encargan de resolver los incidentes y de aportar soluciones para prevenirlos.

1.5.4 Herramientas de un SOC

No existe un estándar o un paquete de software determinado con todas las herramientas de un SOC. Se utilizan herramientas para obtener toda la información sobre la actividad en la organización para utilizando sistemas de gestión de eventos e información de seguridad, se monitorice y analice dicha actividad en busca de amenazas que afectan a la red de la organización.

Existen soluciones empresariales muy completas para grandes organizaciones, cuyos precios no entran en el presupuesto de it de pequeñas y medianas organizaciones. Pero también existen herramientas open source con las que poder implementar un SOC con todas las garantías de cubrir sus necesidades, este trabajo de fin de master se centrara en este tipo de solución para poder englobar el mayor número de organizaciones posibles a las cuales este trabajo le sea de utilidad.

1.5.5 Estándares de un SOC

Tampoco existe un estándar de normas para un SOC, aunque tienen estructuras comunes, no existe una estructura igual para todos los SOC's no hay una norma que diga cómo deben ser ni las funciones que deben cumplir, por ello los SOC's se ven afectados por las normas y estándares que regular la ciberseguridad de todo una empresa, ya que son parte de la ciberseguridad de la empresa, por ejemplo la ISO 27001 [4]establece los requisitos para la implantación de un sistema de gestión de la seguridad de la información (SGSI) y la ISO27002 establece una guía de buenas prácticas para la seguridad de la información. La norma NIST SP 800[5] establece diferentes guías para la

[4]https://www.aenor.com/certificacion/tecnologias-de-la-informacion/seguridad-informacion

[5] https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

respuesta a incidentes de seguridad. La agencia ISA establece el ISA/IEC 62443[6] establece normas para la seguridad de los sistemas de control y automatización industriales, el RFC 2196 [7]es una guía para el desarrollo de políticas y procedimientos de seguridad para sistemas de información. Como se puede ver existen numerosas guías y estándares para la gestión de incidentes, para políticas de seguridad y de buenas prácticas en general, todos de una forma y otra afectan al SOC porque es parte de la gestión de la seguridad en una organización, pero no existen normas específicas para él.

1.6 Recursos

Para la realización de este trabajo de fin de master, además de la inversión de tiempo y esfuerzo, la paciencia y comprensión de la familia, y la total colaboración de mis jefes se dispondrá de los siguientes recursos:

- Portátil de trabajo con el cual se configurará las herramientas del SOC y se realizarán pruebas.
- PC personal donde se redactará la memoria y se realizará la investigación teórica.
- PC con una placa madre X89 con un amd opteron de 8 nucleos, 20g de ram, 256g de disco duro ssd y un disco duro mecánico de 1T para almacenar la información. En este pc será donde se instalen todas las herramientas del SOC y se integrará en la red de la empresa.
- Software open source seleccionado en la fase practica para la implementación del SOC.
- Las instalaciones de la organización colaboradora.

[6]https://www.isa.org/training-and-certification/isa-certification/isa99iec-62443/isa99iec-62443-cybersecurity-certificate-programs
[7] https://en.wikipedia.org/wiki/Site_Security_Handbook

2. Introducción al SOC

2.1 ¿Qué es un SOC?

Un Centro de Operaciones de Seguridad (SOC), se compone de un grupo de profesionales que monitorizan, previenen y controlan la seguridad de las redes de una organización, se encargan de continuamente estar monitorizando dichas redes para realizar un seguimiento y analizar la actividad en los elementos de la organización a proteger, como servidores, sitios web, aplicaciones, bases de datos y demás elementos que son considerados posibles objetivos de ataques y puedan comprometer la continuidad de negocio, en busca de comportamientos anómalos. Un SOC dispone de los medios tecnológicos para visualizar, detectar y detener un incidente de seguridad utilizando sus sistemas de detección, correlación y predicción.

Según el tipo de red e infraestructuras que proteger hay muchos términos para denominar a un centro de defensa de redes informáticas.

- Equipo de Respuesta a Incidentes de Seguridad Informática, *Computer Security Incident Response Team* (CSIRT)
- Equipo de respuesta a incidentes informáticos, *Computer Incident Response Team* (CIRT)
- Centro de respuesta a incidentes informáticos, *Computer Incident Response Center* (CIRC)
- Centro de Respuesta a Incidentes de Seguridad Informática, *Computer Security Incident Response Center* (CSIRC)
- Centro de Operaciones de Seguridad, *Security Operations Center* (SOC)
- Centro de Operaciones de Ciberseguridad, *Cybersecurity Operations Center* (CSOC)
- Equipo de Respuesta a Emergencias Informáticas, (CERTI).

El Centro de Operaciones de Seguridad está diseñado para realizar un seguimiento en tiempo real, dar respuesta a los incidentes de seguridad y cumplir con las normas y estándares exigidos, como por ejemplo la ISO 27001, utilizando las mejores tecnologías en seguridad y los profesionales altamente especializados. Gracias a la evolución de la velocidad de conexión a internet la ubicación del SOC puede variar, puede estar dentro de la organización como SOC local, puede estar en una ubicación distinta incluso en un país distinto y monitorizar las redes de forma remota, o incluso de forma mixta, una parte del SOC trabaja en local y además envía los logs a un SOC externo.

Los integrantes del SOC son profesionales técnicos muy especializados, tanto en la prevención y la defensa de la seguridad de redes y aplicaciones, pero provienen de perfiles diferentes y diferentes disciplinas, Además deben de estar en constante formación para enfrentarse a las nuevas amenazas que surgen. Deben existir diferentes perfiles porque el SOC se organiza con cuatro niveles

2.2 Estándares, normas y guías

No existe una normativa propia para un SOC, cada organización lo implementa según sus necesidades y recursos, lo que si existen son normativas y estándares sobre la seguridad de la información en organizaciones, por lo tanto, como el SOC es una parte de la estructura de seguridad informática se ve afectado por ellas, sin ser concretamente pensadas para él. También existen guías y marcos de trabajo que dan recomendaciones de buenas prácticas e indicaciones de implementación.

2.2.1 ISO/IEC 27001

La normativa ISO/IEC 27001 indica que debe tener un SGSI (Sistema de Gestión de Seguridad de la Información), pero no como se debe de implementar, por ello ISO creo una serie de guías de implementación bajo la misma numeración "ISO 270xx". Dentro de esta norma se especifica por ejemplo como se debe de actuar frente a un incidente de seguridad, como se han de procesar los indicios obtenidos en la auditoría, incluso el procedimiento para contratar un seguro frente a incidentes de seguridad. Esta normativa es global para la organización, pero la mayoría de los elementos que especifica debe tener un SGSI son funciones del SOC, también es ampliamente utilizada como guía de buenas prácticas para la respuesta de incidentes de un SOC y auditorias de la empresa.

Ilustración 1: Esquema de implantación de un SGSI

2.2.2 NIST

El marco de ciberseguridad del NIST (National Institute of Standards and technology de EE.UU) ayuda a las organizaciones a entender los riesgos de ciberseguridad a los que están expuestos, administrar y reducir dichos riesgos, y proteger sus redes y datos. Aporta a las organizaciones una guía de las mejores prácticas en seguridad informática para ayudar a decidir cómo gestionar los recursos económicos y de tiempo en tareas de protección de ciberseguridad.
El Marco de Ciberseguridad del NIST está dividido en estas cinco áreas:

1. Identificación: Se debe listar todos los activos de la organización y aplicarles una política de seguridad que cubra las funciones y responsabilidades de los empleados, proveedores y todo aquel que tenga acceso a datos delicados, además de los pasos a seguir para protegerse contra un ataque y limitar el daño si se produce un ataque.
2. Protección: Deben de implementarse políticas de seguridad para el control de acceso a datos y equipos, copias de seguridad, instalación de software de seguridad, asegurar las actualizaciones del software y formar al personal en temas de ciberseguridad.
3. Detección: Hay que monitorizar los elementos de la red, identificar las posibles anomalías e investigarlas.
4. Respuesta: Ha de existir un plan de respuesta para incidentes de seguridad, que asegure la transparencia de lo ocurrido, la continuidad del negocio y que permita investigar lo ocurrido y la conservación de los indicios.
5. Recuperación: Después de un incidente se debe tener mecanismos para la reparación y restauración de las partes afectadas.

Este marco de trabajo no está pensado directamente para un SOC si no para una organización, pero podría servir para la implementación de un SOC perfectamente, ya que engloba las principales funciones que debe tener. Para la realización de este trabajo de fin de master, se ha utilizado este marco como gran fuente de influencia.

Ilustración 2: NIST marco de trabajo de ciberseguridad

2.2.3 MITRE ATT&CK

Otro marco de trabajo para un SOC es el MITRE ATT&CK. MITRE es una corporación no gubernamental, cuya misión es intentar resolver problemas que contribuyan a un mundo más seguro. En 2013 presento su framework ATT&CK (tácticas, técnicas y conocimiento común de adversarios por sus siglas en inglés) como marco de trabajo para describir y clasificar los comportamientos de los atacantes, basándose en información real obtenida. ATT&CK es una matriz de comportamientos conocidos de atacantes recopilados en tácticas y técnicas, y expresados en varias matrices, así como a través de STIX y TAXII. Esta lista es una representación global de los comportamientos empleados por los atacantes, es útil para la identificación de ataques y su respuesta, para implementar medidas de seguridad que protejan de ataques ya identificados.

Este marco de trabajo, puede ser implementado dentro de un SOC como parte de la inteligencia para la identificación de posibles ataques, comparando las anomalías con filas de la matriz ATT&CK.

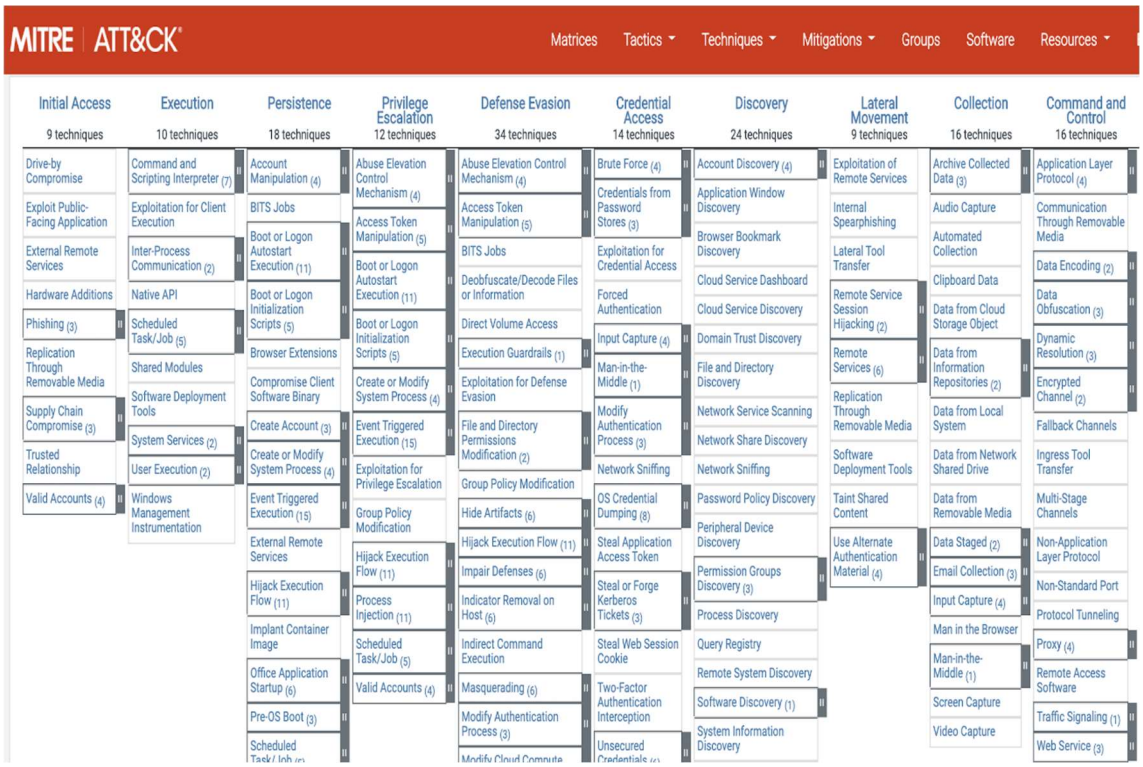


Ilustración 3: Matriz de técnicas y tácticas de MITRE ATT&CK

2.2.4 ENISA

En Europa la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), ha publicado una guía de buenas prácticas para la implantación de un CSIRT y un SOC, esta guía ofrece una orientación basada en experiencias reales, para quienes estén interesados en establecer un equipo de respuesta a incidentes de seguridad informática (CSIRT) o un centro de operaciones de seguridad (SOC), así como orientación para la mejora continua de los diferentes tipos de CSIRT y SOC que existen actualmente. El contenido de este informe se basa en un análisis de las publicaciones actuales sobre la creación de CSIRT; un cuestionario de campo, que fue completado por 40 CSIRT y SOC; y las experiencias de los autores en el establecimiento y la mejora de los CSIRT como parte de numerosos proyectos realizados en Europa, Asia, África y América del Sur.

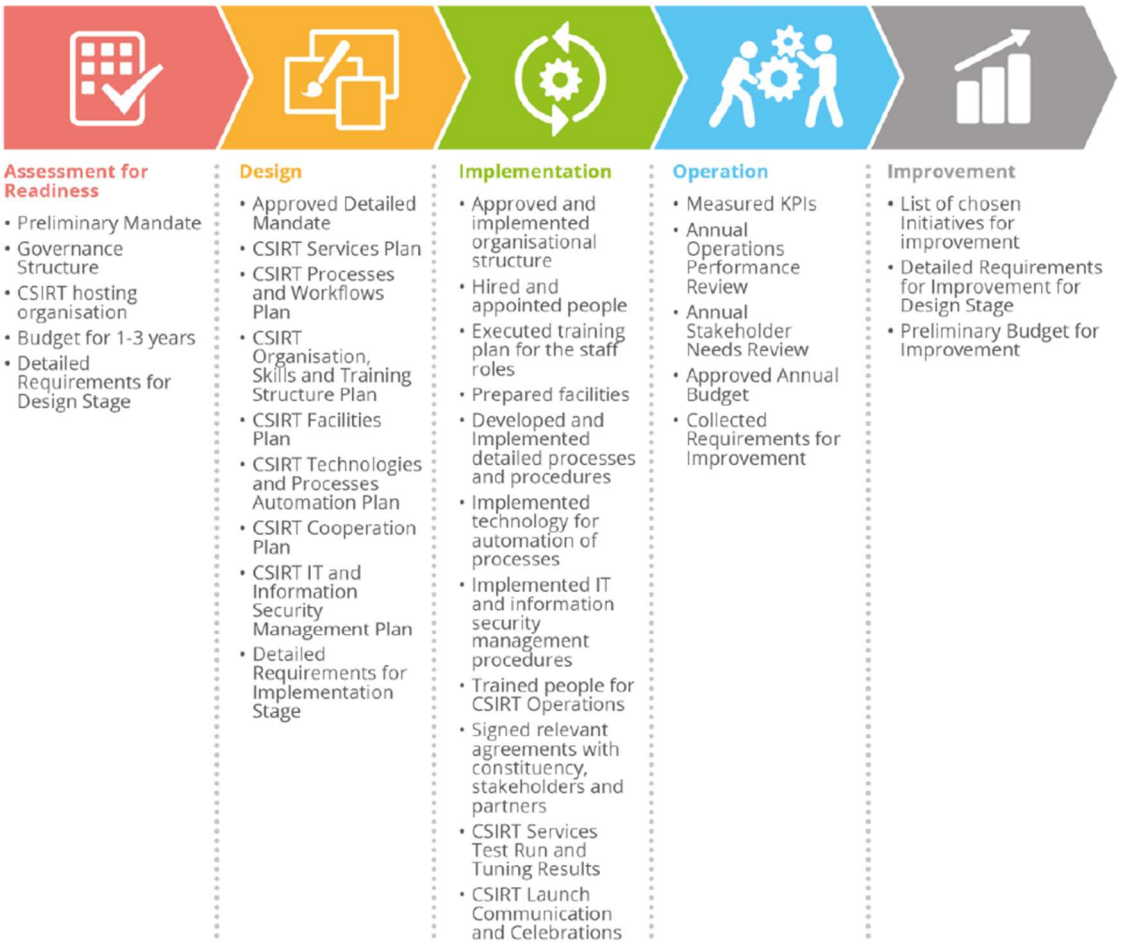


Ilustración 4: Ciclo de implementación de un CSIRT

2.2.5 Esquema Nacional de Seguridad

En España existe el Esquema Nacional de Seguridad (ENS), creado mediante la ley la 40/2015, proporciona al Sector Público un planteamiento común de seguridad para la implementación de un sistema de gestión de seguridad de la información; promueve la mejora continua, fundamental para la transformación a un paradigma digital frente a ciberamenzas; estableciendo un referente de buenas prácticas, promoviendo un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios públicos digitales gracias a los elementos y el lenguaje comunes que han de guiar la actuación de las entidades

En el ENS está recogidas 75 medidas de seguridad divididas en tres marcos.

- Marco Organizativo: Está formado por 4 medidas relacionadas con la organización de la seguridad.
- Marco Operacional: Está formado por 31 medidas, que se deben de tomar para asegurar la continuidad de la operativa.
- Medidas de protección: Está formado por 40 medidas para la protección de los temas y la información.

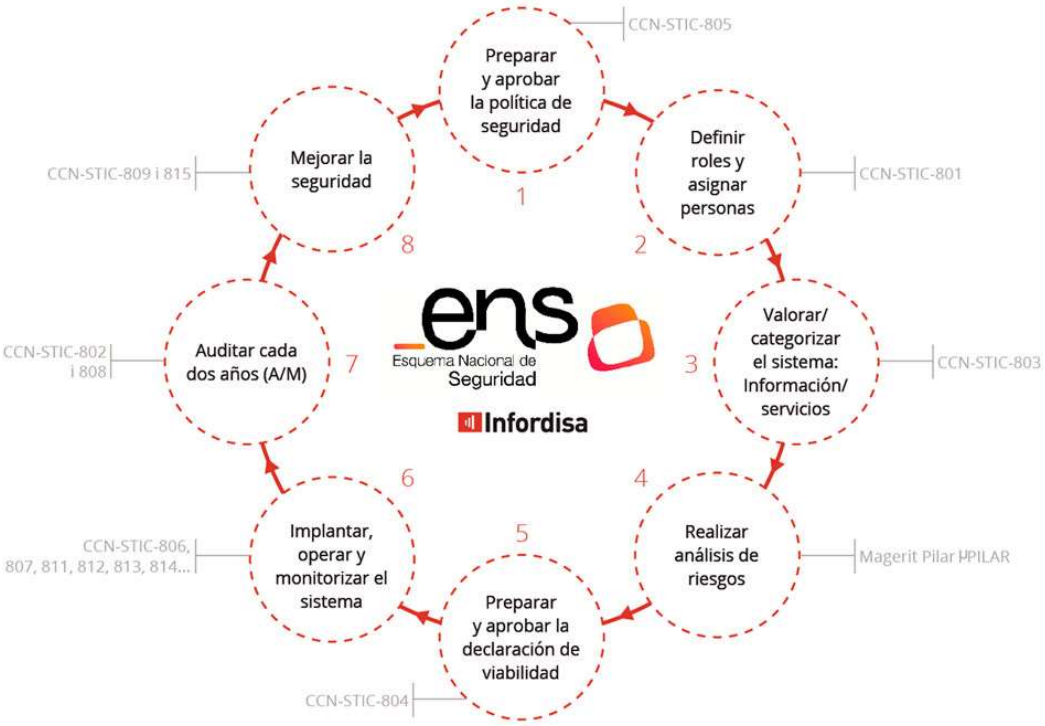


Ilustración 5: Esquema nacional de seguridad[8]

[8] https://www.infordisa.com/es/

2.3 Objetivos y funciones de un SOC

El SOC debe de tener disponibilidad para trabajar durante todo el tiempo que la organización que monitoriza esté activa, normalmente trabaja en 24x7x365, si no pierde su sentido, ya que los atacantes y ciberdelincuentes no descansan ni tienen horario de oficina, el SOC es la primera línea de defensa de los activos de la organización y sus principales funciones son:

- Prevención de incidentes mediante la mejora continua:
  - Análisis de amenazas
  - Escaneo de redes y hosts en busca de vulnerabilidades
  - Coordinación del despliegue de contramedidas
  - Consultoría de política y arquitectura de seguridad.
- Monitorización, detección y análisis de posibles incidentes de seguridad utilizando sistemas inteligentes de análisis.
- Dando respuesta a los incidentes de seguridad, aplicando medidas necesarias para paliarlos.
- Prevenir ataques mediante la formación al personal de las organizaciones a las que se protege.
- Implantar e implementar tecnologías como el IDS y sistemas de recopilación/análisis de datos. análisis de datos.

2.3.1 Principales servicios

Para cumplir con las funciones de SOC se ha de crear un plan de servicios donde se explica los servicios que el SOC presta a una organización, enmarcados en los planes de la organización y en los recursos destinados a este fin.

Ilustración 6: Marco de trabajo para los servicios de first.org

FIRST[9] (Forum of Incident Response and Security Teams) es una asociación global de los CSIRTs, tiene como objetivo principal promover la cooperación y coordinación en la prevención de incidentes. La pertenencia a FIRST permite a los equipos de respuesta a incidentes responder más eficazmente a los incidentes de seguridad, tanto de forma reactiva como proactiva. FIRST reúne a una variedad de equipos de respuesta a incidentes de seguridad informática de organizaciones gubernamentales, comerciales y educativas.

FIRST ha creado un marco de trabajo que detallan los posibles servicios que pueden prestar los CSIRT, en este marco se definen cinco áreas donde se organizan los servicios:

- Gestión de los eventos de seguridad: (Information Security Event Management) En esta área se engloban los servicios de monitorización y detección, además del análisis de eventos.
- Gestión de incidentes de seguridad: (Information Security Incident Management) En esta área están los servicios de análisis y gestión de incidentes, mitigación de ataques y respuesta.
- Gestión de vulnerabilidades: (Vulnerability Management) Esta área están los servicios de recepción de informes de vulnerabilidad, cribado y procesamiento de informes de vulnerabilidad.
- Estado actual: (Situational Awareness) Está área están los servicios de Adquisición de datos, Análisis y síntesis, además de los mecanismos de comunicación de lo que ocurre en el SOC
- Transferencia de conocimientos: (Knowledge Transfer) Está es el área encargada de los servicios de sensibilización, formación y educación del personal de la organización.

Este marco ofrece una lista de directrices para la preparación del plan de servicios del CSIRT.

1. El CSIRT debería echar un vistazo a la última versión del Marco de Servicios CSIRT de FIRST.org. Este documento presenta el mapa conceptual de los servicios CSIRT.
2. De las cinco áreas de servicio, el responsable del SOC ha decidir qué servicios exactos debe proporcionar el SOC para cumplir con las directrices marcadas por la dirección, con los recursos de los que dispone.
3. Seleccionar y ajustar los nombres de las áreas de servicio, ya que los nombres proporcionados en el Marco de Servicios del CSIRT pueden ser demasiado detallados inicialmente.
4. Validar la lista de servicios resultantes para garantizar que se cubren todas las directrices de la dirección. Los recursos del SOC son limitados; por lo tanto, el director del SOC los debe optimizar para cumplir con la calidad de los servicios ofertados.

La lista de servicios elegidos debe figurar en un catálogo de servicios SOC. Se debe garantizar que el SOC preste de servicios de calidad y, si estos servicios

[9] Computer Security Incident Response Team (CSIRT) Services Framework https://www.first.org

se interrumpen, se recuperen rápidamente. Además de que están en continua mejora a través de la información de las auditorias.

2.4 Estructura de un SOC

Para cumplir con la lista de servicios un SOC se organiza en niveles según su grado de especialización y formación, cada nivel tiene asignadas sus propias funciones. Hay muchos tipos de organización de un SOC, aquí se presenta una estructura organizativa típica con responsabilidades funcionales.

Ilustración 7: Ejemplo de estructura en un SOC pequeño

2.4.1 Supervisor del SOC

El supervisor del SOC es quien se ocupa de la gestión del equipo, del presupuesto y del diseño de los servicios que ofrece. El supervisor tiene entre sus funciones relacionarse con los responsables de la organización y ser el punto de referencia y enlace para la información de los incidentes críticos. Es el máximo responsable del SOC, se encarga de diseñar y mantener actualizado el catálogo de los servicios y optimizar el rendimiento del equipo, también es el roll que gestiona los recursos humanos del SOC, turnos, vacaciones, salarios etc. También el presupuesto. Por ello, es un roll que debe tener cualificación en la gestión de equipos y proyectos, además de debe estar cualificado para la gestión de respuestas ante incidentes de seguridad.

2.4.2 Analista Nivel 1

Los analistas de monitorización del nivel 1 monitorizan constantemente las alertas y las amenazas que se producen en la organización. Su principal trabajo es basándose en la información recopilada cribar las alertas e investigarlas para determinar si estas posibles amenazas se pueden convertir en un incidente de seguridad, y recopilar datos y generar el contexto necesario antes de pasar la alerta al nivel 2. Este roll debe tener una formación en los procedimientos de cribado y detección de anomalías, que pongan en peligro la seguridad de la organización.

Los perfiles que suelen trabajar en este nivel son el ingeniero de sistemas, encargado de la integración de las configuraciones y auditoría en los sistemas de la organización, para que el otro perfil del nivel, el experto de monitorización, pueda monitorizar lo que ocurre en una organización. El experto en monitorización, además de monitorizar responsable de agregar trazas de múltiples fuentes identificando comportamientos anómalos. Estos dos perfiles según el tamaño del SOC pueden coincidir en el mismo profesional.

2.4.3 Analista Nivel 2

El personal del nivel dos es responsable de la respuesta a las alertas provenientes del nivel uno. En este nivel los profesionales tienen una formación y experiencia mayor. El incidente se analiza utilizando unos procedimientos y metodologías definidos en el SOC, además correlando la información con diferentes fuentes de inteligencia, para determinar si hay sistemas críticos involucrados y el alcance del impacto en los datos de la organización. Una vez realizado el análisis eleva posibles soluciones al incidente y proporciona servicios de auditoría del incidente. Para una correcta correlación de datos es fundamental disponer de una cyberinteligencia bien construida y entrenada que aporte información, alimentada tanto por el histórico de datos como por redes de inteligencia global, con las que se comparta información mutuamente. Además de tener sistemas de análisis eficientes y potentes.

El perfil de ingeniero de seguridad es el nivel dos es el de analista experto en seguridad con conocimientos de análisis forense, para identificar mediante la información obtenida como ocurrió un incidente de seguridad, identificando los sistemas comprometidos y el modus operandi del ataque, para poder implantar las medias necesarias para paliarlo y que no se vuelva producir. En este nivel están los expertos en diferentes materias, estos expertos deben estar formados en análisis avanzado forense de redes, metodologías para la respuesta a incidentes, análisis de malware, e inteligencia de amenazas.

2.4.4 Analista Nivel 3

El personal del nivel tres tiene un muy alto, suelen ser especialistas de algún campo o marca concreto, tienen dos funciones principales, recibir las alertas del nivel dos para resolver incidentes de alto nivel y el análisis forense, además de realizar labor preventiva realizando auditorías técnicas, para proponer futuros planes de acción para la mejora continua.

El analista tiene un profundo conocimiento de la red, de los sistemas endpoint, de inteligencia de amenazas, de forense, e ingeniería inversa de malware, y del funcionamiento de aplicaciones y de la infraestructura TI. Están implicados en el desarrollo y mejora de los sistemas de inteligencia analítica.

2.4.5 Administrador de sistemas del SOC

Todos los sistemas de recolección de datos, análisis y monitorización deben de ser administrados y mantenidos, por ello es necesaria la presencia de la figura de un administrador de sistemas que se ocupe que todo funcione correctamente, mantener los sistemas en funcionamiento y actualizados, también ayudando en el diseño e implementación del SOC desde el punto de vista de sistemas.

2.4.6 Estructura final de un SOC

Una estructura típica de un SOC sería la que describe la figura 8

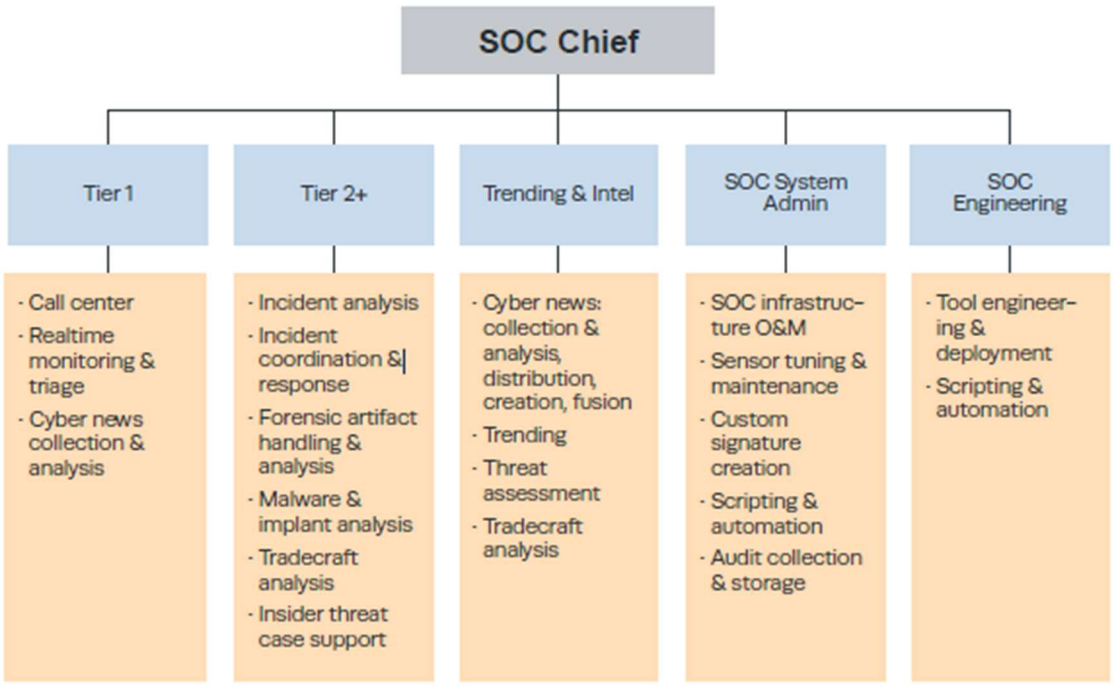


Ilustración 8: Funciones dentro de un SOC

2.5 Modelo operativo de un SOC

La principal tarea de un SOC es la detección y resolución de incidentes de seguridad, según la Norma ISO2701 Anexo A.16, en el manejo de un incidente se han de considerar cinco pasos claves.

Ilustración 9: Pasos para el manejo de un incidente de seguridad

2.5.1 Fases para el manejo de un incidente

Las principales fases para el manejo de un incidente son:

- Fase 1 Notificación del incidente: La organización debe de tener unos procedimientos establecidos para la notificación de un incidente de seguridad, bien por personal de la organización (mail, software de creación de tickets, telefónica, etc.), o por parte del personal de primer nivel del SOC.
- Fase 2 Clasificación del incidente: los profesionales del nivel uno realiza un cribado de la información que les llega y clasifican el incidente.
- Fase 3 Tratamiento del incidente: Un Experto del nivel dos recibe el aviso de un incidente, lo analiza y aplica las medidas necesarias para su resolución.
- Fase 4 Cierre del incidente: una vez el incidente está resuelto se procede a su cierre, se almacena la información generada durante el análisis y su resolución, además de notificar a la persona que lo informo de que se encuentra resuelto.
- Fase 5 Base de conocimiento: Toda la información generada durante el incidente se clasifica y almacena, ampliando la base de conocimiento de los sistemas de detección para mejorar futuras detección y medidas de seguridad.

Siendo esta la principal tarea de un SOC es lógica que su organización interna siga esta estructura.

2.5.2 Fases 1 y 2

Para cumplir con las dos primeras fases del tratamiento de un incidente, en el nivel uno el analista monitoriza la red en busca de anomalías y eventos que puedan indicar el inicio de un ataque, esta monitorización es alimentada por múltiples fuentes (Firewalls, IDS/IPS, Sensores, Antivirus, etc.), debido a la cantidad de información el procesamiento en bruto de todos los eventos por un humano es completamente inviable, es aquí donde entran las herramientas de análisis y correlación de la información llamadas SIEM (Security Information and Event Management), Estas normalizan el conjunto de los datos recibidos, los almacenan y analizan relacionándolos con reglas establecidas y correlacionándolos entre ellos, para intentar detectar incidentes y eliminar falsos positivos. El analista monitoriza la información del SIEM y clasifica los resultados y los provee de un contexto, avisando a los analistas de nivel dos en caso de detectar una amenaza.

2.5.3 Fase 3

La siguiente fase del tratamiento son responsabilidad de los analistas de nivel dos, quienes estudian el incidente en su contexto utilizando herramientas forenses para determinar, la metodología utilizada por el atacante, los sistemas afectados y el alcance dentro de la organización.
El analista de nivel 2, quien a su vez informa al responsable del SOC, quien decide qué pasos hay que tomar, si es necesaria la intervención de un analista de nivel 3, las medidas a tomar para responder al incidente y restablecer los sistemas, o no hacer nada y continuar monitorizando el incidente, dependerá de muchos factores.

- Hay que asegurar que la respuesta no tenga un impacto mayor que el incidente sobre la continuidad de negocio (apagar sistemas imprescindibles, detener totalmente la actividad, etc.)
- Es posible que sea más productivo monitorizar el ataque para comprender mejor la intrusión realizando un análisis forense una vez el intruso ya no está presente.
- Asegurar que es un ataque y no, aunque sea un comportamiento anómalo, corresponde al funcionamiento legítimo de algún sistema.

2.5.4 Fase 4 y 5

Una vez resuelto el incidente de seguridad, se llevan a cabo las dos últimas fases del tratamiento, se cierra la incidencia y la información obtenida se almacena en el SIEM para mejorar la detección de posibles ataques y afinar las reglas para evitar falsos positivos.

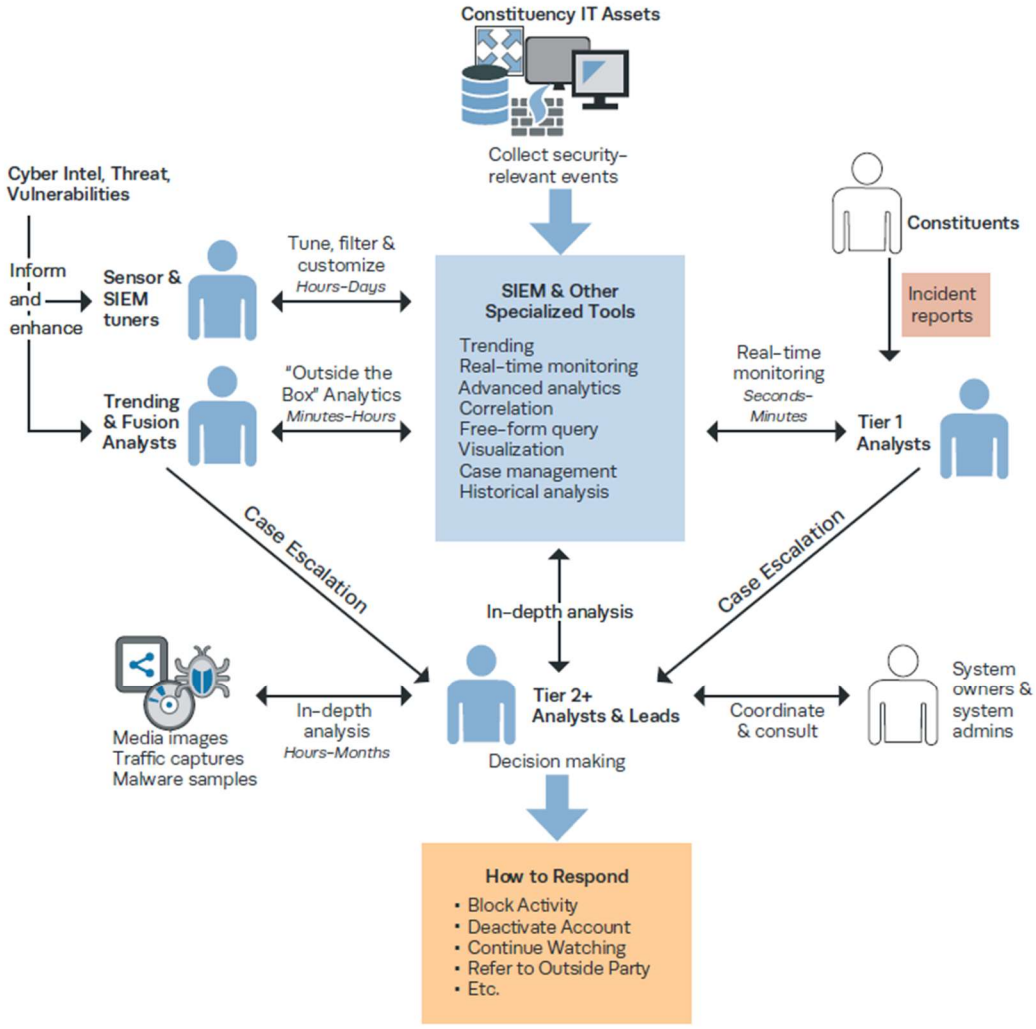


Ilustración 10: Estructura y flujo de trabajo de un SOC

2.6 Herramientas de un SOC

Para el trabajo en el SOC se utilizan un gran número de herramientas, dependerá del tamaño del SOC, pero las que seguro podemos encontrar por ser las básicas para su funcionamiento son estas.

2.6.1 IDS / NIDS / IPS

Un IDS (Intrusion Detection System) es una herramienta para la detección de acceso no autorizados a una red o sistema, generando una alerta o log para que sea revisador por un analista del SOC. El IDS únicamente alerta de un posible ataque, no realiza ninguna acción de contramedida. A diferencia de un IDS un IPS (Intrusion Prevention System), que también se utilizan para la protección de una organización en un SOC, al detectar la intrusión realiza una acción programada según el tipo de ataque, para prevenirlo o incluso llegar a mitigarlo.

Para la detección de amenazas los IDS se basan en el uso de reglas, analiza el tráfico de red y cuando una consecución de eventos cumple una de las reglas crea un aviso. Estas reglas pueden ser creadas por el personal del SOC como

parte del conocimiento adquirido en otros ataques, o aportadas por la comunidad como parte del conocimiento colectivo.

Según la arquitectura de red del IDS se pueden dividir en dos tipos:
HIDS (HostIDS): Cuando el IDS únicamente monitoriza un equipo, está conectado entre la red y un host específico, analizando todo el tráfico entrante y saliente.
NIDS (Network IDS): En esta arquitectura el IDS se comporta como un sniffer, está conectado a la red capturando todo el tráfico y alertando si algún equipo genera tráfico anómalo.

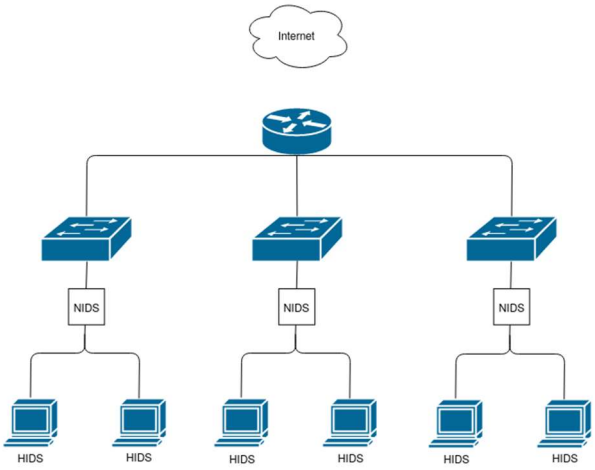


Ilustración 11: Esquema de red de NIDS y HIDS

2.6.2 SIEM

Un SIEM (Security Information and Event Management) es seguramente la herramienta más importante de un SOC, su tecnología permite detectar rápidamente amenazas, e intervenir, ya que aporta una visión global de todo lo que ocurre en la red. Los SIEM son fruto de la unión de dos tecnologías diferentes.

SEM (Security Event Management): Centraliza la recepción de eventos en tiempo real desde los diferentes sensores, los procesa y monitoriza, correlacionándolos y generando alertas si encuentra anomalías.

SIM (Security Information Management): Almacena todos los eventos recibidos, para disponer de un histórico de lo ocurrido, permitiendo el análisis forense de incidentes y la generación de conocimiento sobre las metodologías de los atacantes, mejorando su detección.

La importancia de esta herramienta es que permite la detección y prevención de amenazas, pero sobre todo de las amenazas no relacionadas con vulnerabilidades conocidas de software, malware o ataques de denegación de servicios, ya que estas son las más difíciles de detectar. Esto se consigue gracias a la recopilación de información, que permite mejorar las capacidades de identificación e investigación.

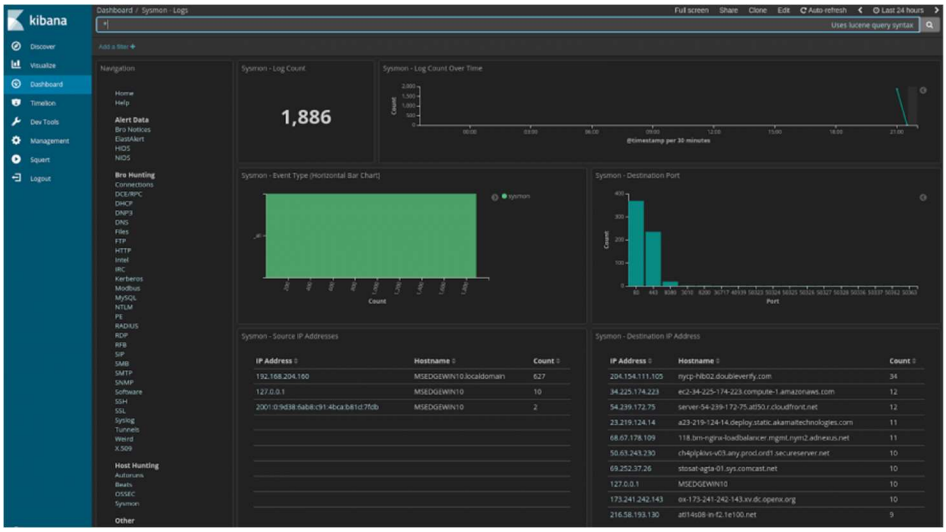


Ilustración 12: Ejemplo de dashboard de un SIEM

El flujo de trabajo de un SIEM es el siguiente:

- Recolección de la información: Recoge los logs de los eventos provenientes de los sensores y agentes instalados en los equipos y en la red.
- Normalización de los logs: Para que se puedan crear reglas y correlacionar los datos estos tienen que tener el mismo formato, pero los logs recogidos por el siem tienen el formato que le dio el dispositivo que los creó (CSV, XML, JSON etc.). El SIEM debe extraer la información y normalizar el formato.
- Correlación de los datos: Una vez obtiene los datos normalizados son inyectados en el motor de correlación en tiempo real donde se les aplican las reglas definidas, estas reglas pueden desencadenar acciones como la creación de un caso para su análisis, adjuntándole el evento, o sistemas más complejos incluso cambiando las reglas del firewall.
- Almacenamiento de los datos: Los datos ya analizados son almacenador para disponer de un histórico de eventos, que permita futuros análisis forenses, y ampliar la base de conocimiento del SIEM.

Ilustración 13: Flujo de trabajo de un SIEM

2.6.3 Escáner de vulnerabilidades

Las vulnerabilidades en el software es uno de los principales puntos de ataque, igual que los servicios mal configurados o exponer puertos TCP/UDP a internet sin estar protegidos por un firewall. Un escáner de vulnerabilidades es un software diseñado para realizar análisis automáticos recogiendo información sobre los servicios en funcionamiento, los puertos abiertos, fallos de configuración, posibles vulnerabilidades conocidas en el software del equipo o servidor facilitando el trabajo a los investigadores e ingenieros del SOC. Se pueden realizar escaneos desde la red interna para buscar los posibles puntos de fallo que se encontraría un atacante si consiguiera acceso a la red, o escaneos desde la red externa para encontrar posibles vulnerabilidades expuestas a internet.

Existen diferentes tipos de escáneres según el tipo de vulnerabilidades que auditan.

- Basados en host: Escanea un host o sistema, se ejecutan en el sistema objetivo rastreando los eventos e informando del análisis de seguridad.
- Basados en red: Escanea los equipos de una red, detectando sistemas operativos, los puertos abiertos e identifican servicios que se ejecutan en esos puertos, revelando posibles vulnerabilidades asociados a estos servicios.
- Basados en web: Escanean aplicaciones web en busca de vulnerabilidades (sql injection, script injection, Cross-Site Scripting (XSS)).
- Basados en base de datos: Escanean bases de datos detectando inseguridades, utilizando herramientas y técnicas para evitar vulnerabilidades.

Normalmente se utiliza una combinación de escáneres para cubrir todo el espectro de vulnerabilidades, host, red, portales web de la organización. Existen herramientas que recompilan diferentes escáneres y automatizan los procesos.

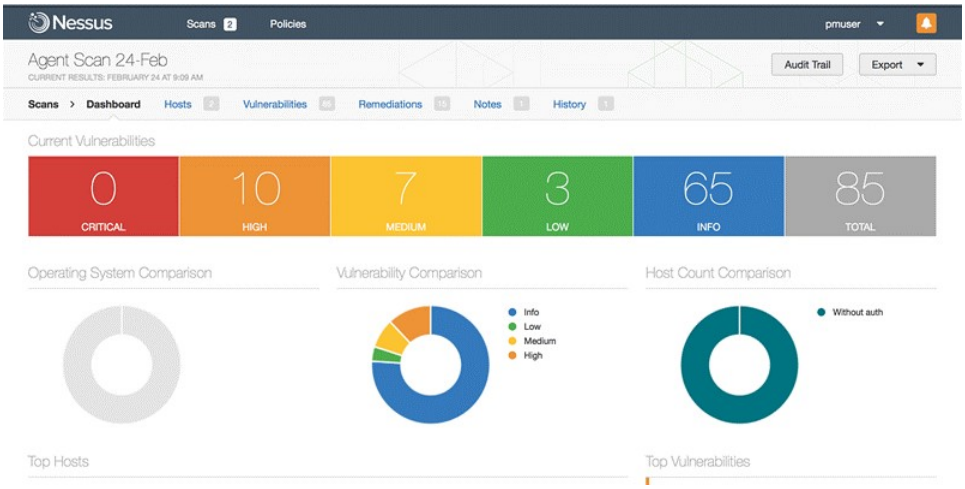


Ilustración 14: Resultado de un escáner de vulnerabilidades (Nessus)[10]

[10] https://es-la.tenable.com/products/nessus

2.6.4 Herramientas de captura de paquetes y forenses.

Existen herramientas especializadas en la adquisición y almacenamiento del tráfico, para el seguimiento de los incidentes y la investigación forense del ataque. El disponer de los paquetes de datos enviados durante un ataque permite entender como se ha producido el ataque la metodología utilizada por el atacante, además de poder realimentar las herramientas de análisis para la detección de futuros comportamientos anómalos. Estas herramientas almacenan los datos en un formato eficiente y automáticamente eliminan el tráfico antiguo para no saturar el servidor de almacenamiento.

Para poder realizar el análisis se necesitan herramientas forenses, que faciliten el análisis del tráfico, ayuden a buscar patrones y datos relevantes, analizar el tráfico cifrado, además de presentar los datos extraídos. La forma en que se presentan los datos no sólo simplifica el análisis, sino que también ahorra un valioso tiempo al analista o al investigador forense.

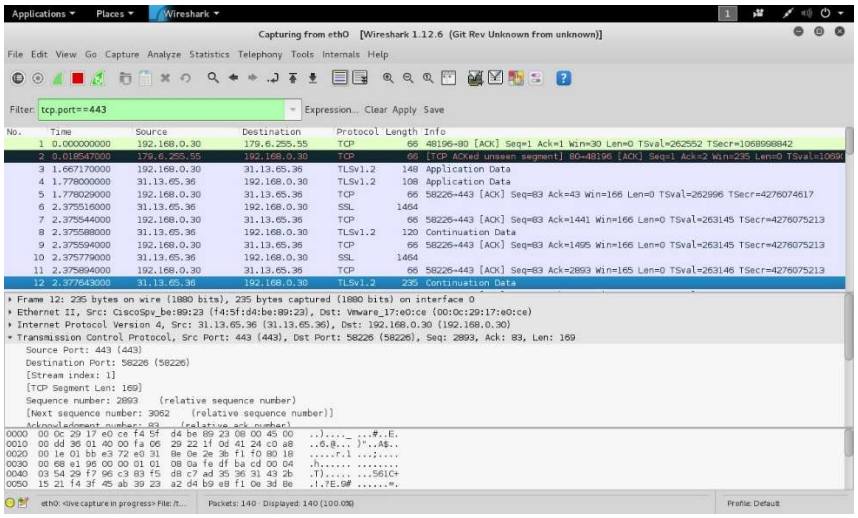


Ilustración 15: Análisis de paquetes con Wireshark[11]

2.6.5 El conjunto de las herramientas.

No existe una estructura típica de un SOC, por lo tanto, las herramientas que utilizaran dependerán de su estructura, tamaño y servicios que ofrezca. Nos podemos encontrar con un SOC que no utilice alguna de estas herramientas, pero por norma general, en la mayoría de ellos están todas presentes, ya que es justamente la unión de todas ellas es lo que dota a un SOC de sus capacidades para cumplir con los servicios que ofrece.

[11] https://www.wireshark.org/

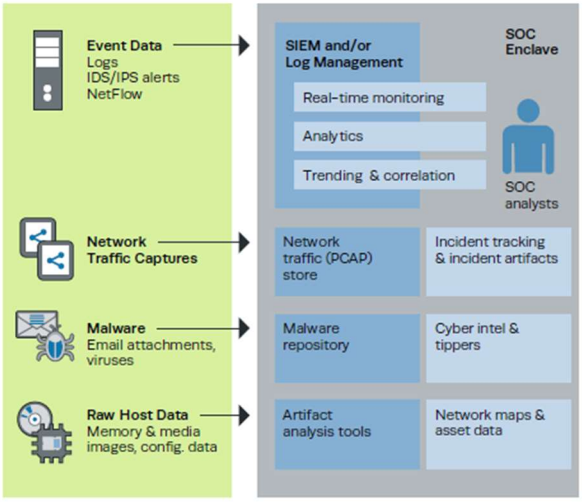


Ilustración 16: Herramientas de un SOC

2.7 Aspectos previos a la implantación de un SOC

La implementación de un SOC es necesaria para que una organización sea capaz de detectar y resolver un incidente de seguridad. Si una organización toma la decisión de establecer un SOC, la primera pregunta importante que se debe de contestar es: ¿Qué tenemos que hacer para realizar esta implantación dentro de mi organización con la mayor eficacia? Se ha de ser crítico y consciente con los recursos de los que se dispone, para poder responder a esta pregunta. Por ejemplo:

- ¿Se dispone de tecnologías que pudieran ser de utilidad ya presentes en la organización?
- ¿El equipo del SOC tiene a su disposición estás tecnologías?
- ¿Cuál es la preparación del actual equipo del SOC?
- ¿Qué recursos de tiempo actualmente pueden dedicar los integrantes del SOC?
- ¿Cuál es la prioridad que la dirección de la organización le da a este proyecto?

Comprender estas restricciones y darles respuesta a estas preguntas, es uno de los objetivos de este proyecto, que se irán teniendo en cuenta a lo largo del trabajo, para poder asegurar que se realice una implantación efectiva y continuada en el tiempo. Son cuestiones importantes porque si por ejemplo ya existen equipos útiles para el SOC en la organización, pero no se puede garantizar el acceso a los datos que generen por políticas, no resultan de ninguna utilidad. Igualmente, si se aportan todos los recursos económicos necesarios por parte de la organización para la adquisición de equipamiento y tecnología, pero las capacidades del equipo, ya sea por falta de formación capacidad o tiempo, no son capaces implantarlas, integrarlas o gestionarlas, son recursos desaprovechados, es más eficiente primero formar y confeccionar un equipo a la altura y después adquirir las tecnologías necesarias.

2.7.1 Hoja de ruta y planificación temporal para la implementación de un SOC

Antes de la implementación de un SOC se ha de ser consciente que es un trabajo largo, no consiste en instalar las herramientas y comenzar su operatividad. Se ha de crear una hoja de ruta que debe incluir un calendario previsto para las fases de establecimiento del CSIRT -diseño, implementación y operaciones- y otras iniciativas de mejora.

Ilustración 17: Hoja de ruta para la implementación de un SOC

Las fases para la implementación de un SOC son las siguientes:

1. Evaluación (2-12 meses): Esta fase se da sobre todo en CSIRT dependientes de un gobierno o una institución pública. En esta fase se establecen la organización, el órgano de gobierno y los requerimientos de diseño.
2. Diseño (3-6 meses): Formar el equipo, construir el SOC, obtener el apoyo de la organización, establecer políticas en la organización.
3. Implementación (3-12 meses): Establecer los servicios que se va a ofrecer, el organigrama del equipo, instalar los equipos, el equipo formado comienza a trabajar.
4. Capacidad operativa inicial (12 -18 meses): Debería de tener las herramientas adquiridas parcialmente en funcionamiento, el equipo básico formado y el SOC comienza a trabajar con algunos de los servicios operativos.
5. Capacidad operativa completa (a partir de 18 meses): El SOC está en completo funcionamiento, el equipo está completo.

2.8 Organización y herramientas de nuestro SOC

Una vez definido lo que es un SOC, las funciones que realiza y las partes que lo componen, toca definir la organización del SOC que se va a implementar es mi empresa y las herramientas a utilizar, teniendo en cuenta los recursos y la estructura de la empresa.

2.8.1 Estado previo de la organización

La empresa tuvo un incidente de seguridad en el año 2015, sufrió el ataque de un ransomware, por suerte se pudo desencriptar toda la información. A partir de ese momento se empezaron a tomar medidas, se cambiaron los programas a gestión a la nube y se comenzó a utilizar almacenamiento compartido en nube. Después en una segunda fase se instaló un firewall perimetral, endpoints de antivirus en todos los equipos, un servidor de copias de seguridad, políticas de seguridad, formación a los empleados y auditorías externas. Aun no se dispone de un sistema de gestión de la seguridad de la información (SGSI), pero se está trabajando en ampliar las políticas de seguridad y la implantación del SOC es también un avance importante.

2.8.2 Hoja de ruta y requisitos.

La hoja de ruta marcada para la implementación de un SOC en mi organización podría definirse como:

2.8.2.1 Evaluación

Esta fase se ha realizado previamente a este trabajo de fin de master, se ha definido que se necesita un SOC que realice un trabajo de monitorización 8x5[12], pero con posibilidad de aviso de incidente 24x7[13], que sea capaz de monitorizar la actividad en la red de la organización y de los servidores externos, además de realizar formación a los empleados.

2.8.2.2 Diseño

Esta fase es la principal tarea de la parte práctica de este trabajo, al final, tendremos un diseño real de un SOC. Que como primera fase se ocupará de la monitorización de la red local, para en siguientes fases añadir la monitorización de los servidores externos de la organización, un programa de formación para empleados y por último confeccionar un SGSI.

2.8.2.3 Implementación

Esta fase completa la tarea de la parte práctica de es te trabajo, se obtendrá un SOC implementado. La intención es dejar está fase completada con un equipo formado, un servidor con todas las herramientas del operativas, y la lista de servicios definida.

2.8.2.4 Capacidad operativa inicial

Esta fase continua a partir de la finalización de este trabajo, en esta fase se monitorizará la red local de la empresa. Se podrán en funcionamiento las

[12] 8 horas al día, 5 días a la semana.
[13] 24 horas al día, 7 días a la semana.

herramientas implementadas, se instalan los user agents en los hosts y comenzará las tareas de monitorización. Se comenzará la elaboración de un SGSI conjuntamente con otros órganos de la empresa.

2.8.2.5 Capacidad operativa completa

En esta fase se añadirá la monitorización de los servidores externos de la red, se conectarán los sensores con el siem principal para poder monitorizar la actividad del servidor y poder detectar posibles incidentes de seguridad. Además, se iniciarán las tareas de formación del personal de la organización en materia de ciberseguridad. Y se completará la elaboración de un SGSI, quedando pendiente la decisión de obtener la certificación ISO27000.

2.8.3 Organización.

La empresa entiende que la implantación del SOC es un proyecto importante, ya que como operadora de telefonía de ascensores debe asegurar el funcionamiento de sus equipos y la continuidad de negocio de sus clientes, para ello es muy importante disponer de mecanismos de detección y respuesta de incidentes de seguridad. Como recursos del personal para la implementación se dispone del administrador de IT de la empresa y del autor de este proyecto, además de un asesor externo, en estas personas recaerán las funciones y responsabilidades del SOC.

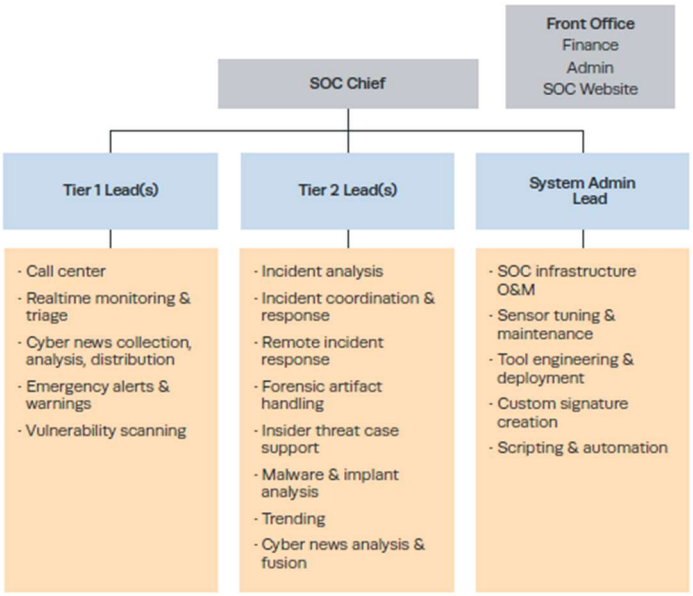


Ilustración 18: Organización de un pequeño SOC

2.8.3.1 Preparación y recursos

La preparación actual y recursos de tiempo del equipo es la siguiente:

- Administrador IT: Tiene un título de Graduado Superior En Administración De Sistemas y un curso de experto en seguridad informáticas. Sus funciones actuales son las del mantenimiento informático de los equipos de la empresa y la administración de los servidores externos, además del despliegue de los servicios desarrollados por I+d+I.
- Autor del proyecto: Realiza este trabajo para obtener el Máster Universitario En Seguridad De Las Tics, además es Ingeniero Técnico de telecomunicaciones y tiene un curso de experto de seguridad. Sus funciones actuales son las de Proyect Manager e ingeniero de desarrollo dentro del departamento de I+d+I, además de ser el responsable de la estructura de servicios y servidores en la nube.

2.8.3.2 Roles y funciones

Basándose en las características y funciones actuales de los miembros del futuro SOC, los roles y responsabilidades se van a repartir de la siguiente forma:

- Administrador IT: Debido a que sus funciones principales ya incorporar el mantenimiento de los equipos y la red, tendrá los roles de analista de nivel 1 y Administrador de la estructura del SOC. Se encargará de monitorizar la actividad de la red y los equipos además del mantenimiento de los servicios del SOC.
- Ingeniero Master MISTIC: Compaginará sus funciones de ingeniero de desarrollo i+d+i, con el rol de analista nivel 2 y responsable del SOC. Se ocupará de la identificación de los incidentes de seguridad y su solución junto con el Administrado de IT, además de servir de enlace con la dirección de la empresa.
- Colaborador externo: Se respaldará el SOC en un colaborador externo que realizará las funciones de analista nivel 3 y como asesor en la mejora continua de la seguridad de la organización.

2.8.4 Herramientas.

El SOC tiene como recurso un servidor que se instalará físicamente en la red de la oficina y donde se ejecutarán todas las herramientas, es lo que se conoce como instalación single server, por ello en lugar de elegir las herramientas una a una, instalarlas e integrarlas se decide instalar un framework especializado, que incluye todas las herramientas necesarias para auditar y monitorizar la red ya integradas entre sí, de esta forma se favorece la estabilidad del sistema y se reduce el tiempo de integración, a pesar de eso la configuración y afinación del SOC sigue siendo un trabajo que hay que hacer.

Dentro de los frameworks disponibles en el mercado la mayoría son de pago, pero uno de los objetivos de este proyecto era implementar un SOC con software open source, asi que buscando entre los proyectos open source se ha realizado una comparativa entre 3.

2.8.4.1 AlienVault's OSSIM

OSSIM, la versión de open source del SIEM de pago USM de AlienVault, posiblemente sea una de las plataformas SIEM open source más conocidas. OSSIM incluye componentes clave de SIEM, a saber, recopilación, procesamiento y normalización de eventos y, lo que es más importante, correlación de eventos.

OSSIM combina las funciones de SIEM con proyectos open source para construir una solución completa. Como por ejemplo FProbe, Munin, Nagios, NFSen/NFDump, OpenVAS, OSSEC, PRADS, Snort, Suricata y TCPTrack.

OSSIM no tiene las mismas funciones que la versión de pago USM. Para organizaciones pequeñas es una solución funcional, pero a gran escala presenta problemas de rendimiento. Por ejemplo, OSSIM prácticamente no tiene capacidades de gestión de logs.

Pros	Contras
Integración de numerosos proyectos open source	No existe una gran documentación para su integración y configuración
Scanner de vulnerabilidades integrado	No dispone de capacidades de gestión de logs
Necesidades de hardware asequibles 16G de ram y 4 cores.	La integración de tickets de incidentes es peor que la competencia.

Tabla 1: Pros y contras de alienvault's ossim

2.8.4.2 Siem Monster

SIEMonster a pesar de ser un proyecto relativamente nuevo se ha convertido en muy popular, se basa en tecnología de open source y está disponible de forma gratuita (community edition) o como solución de pago (Premium, Enterprise y MSSP edition).

SIEMonster utiliza su propia terminología "monstruosa" para nombrar los proyectos de open source que lo integran. Por ejemplo, ELK para la recopilación, el procesamiento, el almacenamiento y la visualización de los datos de seguridad recopilados. SearchGuard se utiliza para el cifrado y la autenticación sobre Elasticsearch y ElastAlert para las alertas.

SIEMonster incluye todas las herramientas que un analista de SOC podría necesitar, accesibles directamente desde un menú principal, por ejemplo, utiliza Kibana para la búsqueda y visualización de datos, MineMeld para la inteligencia de amenazas y Alertas para la creación y gestión de notificaciones basadas en eventos.

Pros	Contras
Integran un gran número de herramientas, todas las que se pudieran necesitar	La versión open source se distribuye como una ova para ser ejecuta sobre una máquina virtual
Existe una gran comunidad y mucha información	Los requerimientos hardware son grandes, como mínimo 32G de ram y un procesador de 8 núcleos, además de las necesidades de la máquina virtual donde se ejecuta.

Tabla 2: Pros y contras de siemonster

2.8.4.3 SecurityOnion

SecurityOnion no es un framework es una distribución de Linux, diseñada para la auditoría de redes y detección de intrusos. Integra otros proyectos open source como ELK Stack, Wazuh, Snort, Suricata y otros. No existe una versión de pago, la empresa que lo mantiene comercializa el soporte y hardware de servidores.

Proporciona múltiples herramientas, IDS's basados en el host y en la red, captura de paquetes completa con netsniff-ng para la monitorización y detección, como otras opciones incluyen TCPDUMP basado en GUI y la interfaz de línea de comandos Wireshark.

Pros	Contras
Dispone de una extensa documentación.	No integra escáner de vulnerabilidades
Permite ejecutar dockers lo que permite la integración de nuevas herramientas.	
Sus requerimientos de hardware son menores que los de 12G y 4 cores.	

Tabla 3:Pros y contras de securityonion

Al final en la integración del SOC se decide por utilizar la distribución SecurityOnion, es la que mejor se adapta al hardware del que se dispone, incorpora todas las herramientas que son necesarias en el SOC y mediante docker es sencillo incorporar nuevas, no es una versión limitada de una solución comercial es un proyecto íntegramente open source, y hay suficiente documentación para completar la integración y configuración del SOC.

3. Estudio de la red de la organización.

El trabajo de un SOC es un trabajo muy complicado, se han de detectar incidentes de seguridad basándose en la información proporcionada por unas pocas y sofisticadas brechas de seguridad. Sin embargo, a grandes rasgos y desde una vista conceptual, el trabajo esencial está bastante definido. Asegurar un entorno consiste en responder a unas pocas preguntas básicas:

- ¿Qué tenemos que proteger?
- ¿Qué activos son vulnerables a ataques?
- ¿Qué es normal? ¿Cómo detectar un ataque sin una sólida referencia de la normalidad?
- ¿Se detectar un incidente de seguridad?
- ¿Cómo automatizo el análisis de los datos?

Responder correctamente a estas preguntas pasa por implementar un sistema que automatizado que permita evaluar los procesos necesarios.

3.1 Red de la organización y fronteras del alcance de las operaciones del SOC

El primer paso es saber que hay que proteger, definir las fronteras del alcance del trabajo del SOC, ¿Qué es lo que hay que proteger?, estas fronteras estarán en constante cambio porque los atacantes son muy creativos, siempre están buscando nuevos métodos de ataque y redefiniendo las formas de pensar. No puedes proteger algo que no eres capaz de definir.

3.1.1 Alcance de las operaciones

Se puede considerar el alcance de las operaciones queda definido por lo siguiente:

Perímetro: Son aquellos elementos en la parte interna de los firewalls, los incidentes de seguridad pueden ser internos al perímetro o externos.

Redes/Subredes: Son las redes y subredes de la organización que están dentro del perímetro, pueden ser físicas, puedes estar basadas en edificios, localizaciones y segmentos o lógicas como grupos, organizaciones y ámbitos.

Endpoints: Son los dispositivos conectados a las redes/subredes de la organización, pueden ser portátiles, pcs de sobremesa, tablets, móviles, servidores, dispositivos iot, impresoras, cualquier cosa conectada a la red de la empresa que pueda ser utilizada maliciosamente para tener acceso.

El SOC como primera tarea debe de conocer perfectamente la estructura de red de la organización y hasta dónde llega el alcance de sus operaciones, debe conocer que activos tiene que proteger, para saber cómo tiene que protegerlos y que actividades debe realizar para securizarlos.

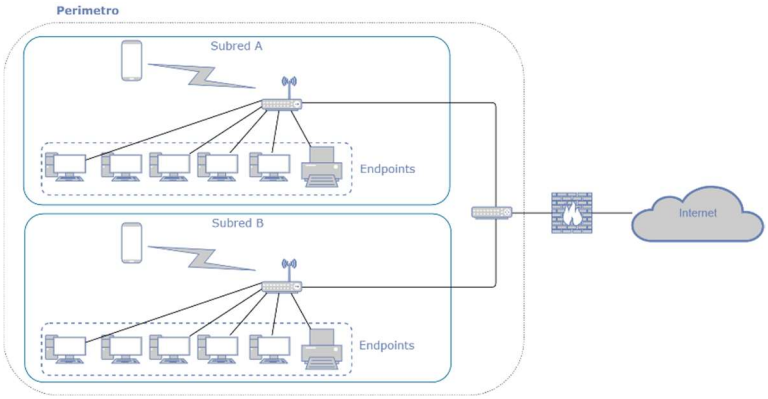


Ilustración 19: Red ejemplo de una organización

3.1.1.1 El trabajo después de la definición de la red

Una vez está definida la red y los activos que la componen ya se sabe que es lo que hay que proteger, ya tiene un punto de partida para tomar decisiones, saber cuánto trabajo puede tener el SOC y que recursos puede necesitar para mantener las fronteras de la organización protegidas.

Pero este trabajo de definición no se hace una vez y ya está, las organizaciones normalmente son entes que están vivos, crecen, cambian y con ellas cambian las fronteras de la red y los elementos que la componen, de esta forma la definición de la red entra en los procesos de mejora continua, según la velocidad de cambio de la organización se debe establecer un periodo de actualización, si la organización es muy estática igual una vez al año es suficiente o si está en constante cambio es necesario hacerlo cada 3 meses.

El conocimiento de la red de la organización por parte del SOC es algo fundamental, si no sabes que tienes que proteger algo es totalmente imposible protegerlo. El personal del SOC debe tener un conocimiento exhaustivo de la red y los elementos que la componen para poder realizar correctamente su trabajo.

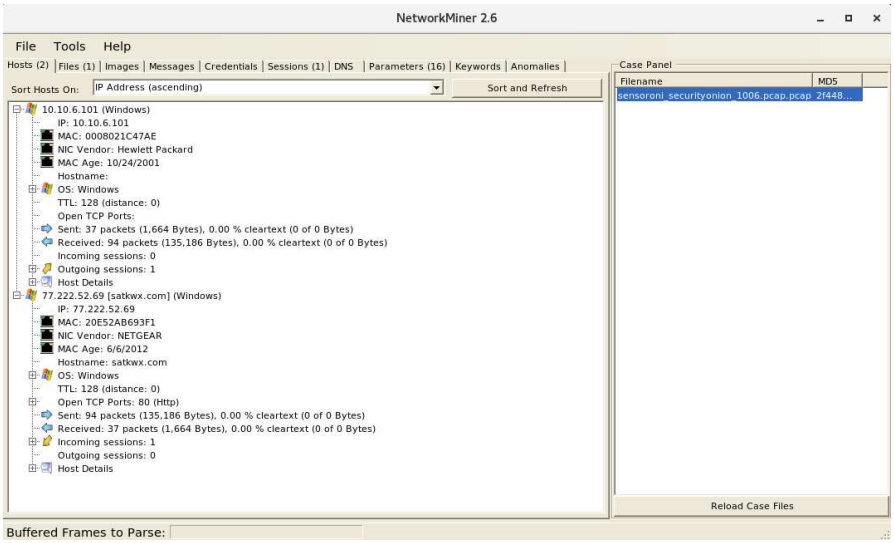


Ilustración 20: Ejemplo de aplicación de descubrimiento de hosts NetworkMiner[14]

[14] https://www.netresec.com/?page=networkminer

3.1.2 Nuestra red

Para implementar el SOC objeto de este proyecto en la empresa donde trabajo, lo primero es realizar un esquema de la red y todos los elementos que la componen. Esta es una simulación de lo que podría ser, por motivos de privacidad no se describe la real.

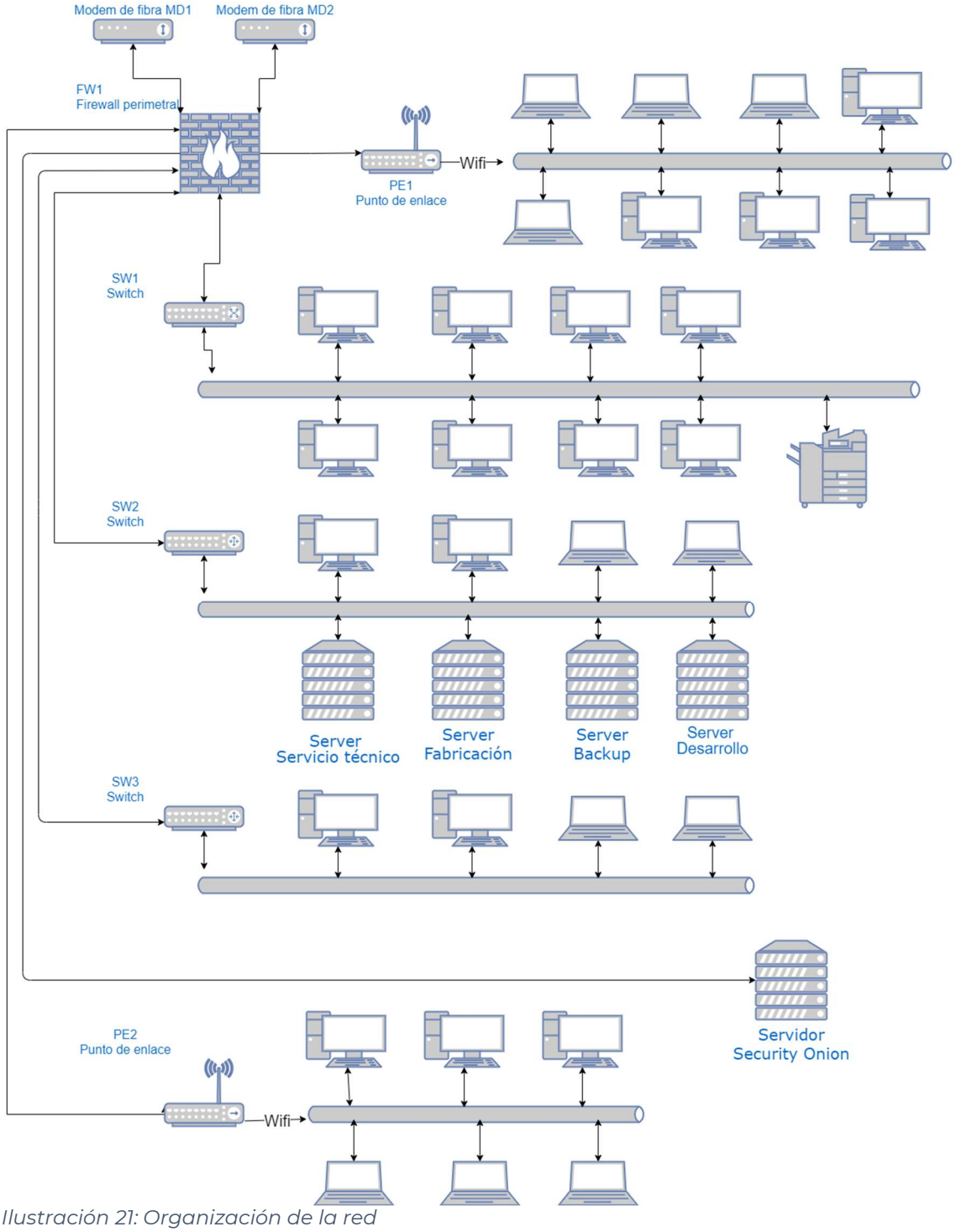


Ilustración 21: Organización de la red

La red está compuesta por:

- Dos módems de fibra óptica que, conectados a la wan del firewall, que hace balanceo.
- Un firewall de cabecera que se ocupa también del ruteo de la red.
- Tres switchs gigabyte que distribuyen la red de cable por la oficina.
- Dos puntos de enlace que generan 3 redes wifi, el PE1 la de invitado y la de la primera planta y PE2 la de la segunda planta.
- Un servidor para desarrollo, donde se prueban los desarrollos y se almacena el repositorio de código.
- Un servidor para fabricación, donde se almacena la información de fabricación (esquemas, firmware, etc) y una base de datos con la trazabilidad de los equipos.
- Un servidor para el servicio técnico, que almacena documentación técnica y la gestión de las consultas e incidencias.
- Un servidor de backup, donde se hacen copias de seguridad de los equipos y servidores locales.
- Un servidor con las herramientas del SOC
- Equipos de trabajo de los empleados de la empresa.
- Fotocopiadora en red.

Este es el organigrama de la red de la empresa, sobre esté esquema se definirán los elementos existentes que pueden ser ya utilizados por el SOC, los principales activos a proteger y la estructura de red donde instalar los sensores y agentes del SOC.

3.1.3 Elementos ya existentes utilizables en el SOC

Una de las primeras preguntas a responder cuando se pretender implantar un SOC en una organización es si existen ya dispositivos en la red que puedan ser utilizados por el SOC, y de qué acceso a ellos se dispone. Esto sirve como punto de partida para empezar a monitorizar información de los eventos conectados a la red y ver que recursos además se necesitan para proteger la red. Si existen equipos que ya ofrecen suficiente información para monitorizar igual con la instalación de un SIEM para la correlación ya se tendría un SOC operativo, si existe, pero por políticas no se tiene acceso hay que buscar otras fuentes de información, o si directamente no existe ninguno hay que plantear la implantación desde cero.

En el caso práctico del proyecto la empresa dispone de un firewall de cabecera y cuatro servidores, de estos 5 elementos ya es posible obtener logs de eventos con los que comenzar. A parte de estos elementos se ampliarán los sensores de información para monitorizar la actividad del resto de equipos.

3.2 Definición de los activos a proteger

Todo sistema de seguridad informática tiene como principal misión asegurar la confidencialidad, integridad y disponibilidad de los datos de la organización. Dentro de las fronteras de la organización existen numerosos objetos que proteger, como equipos, servicios, aplicaciones etc. Se han de identificar todos

estos, las partes que los componen que pueden suponer una amenaza y decidir cuales entran en el ámbito del SOC.
Entender cuáles son los activos que componen una organización es fundamental para optimizar los esfuerzos de cara a un incidente de seguridad y su respuesta. Para un SOC eficaz es necesario ser capaz de priorizar los recursos para hacer frente a las amenazas. Es frecuente que las capacidades de detección de anomalías y las políticas de respuesta se implanten en la organización sin una comprensión real de cómo conseguir obtener el mayor impacto en la empresa. Por ello una parte esencial de los procesos de implantación y mejora continua es tener un profundo conocimiento de los activos existentes en la organización y los servicios que ejecutan en ellos activos.

Además de para poder primar los esfuerzos en relación a su impacto potencial en la organización, conocer profundamente los activos presentes en la organización permite priorizar técnicamente la respuesta a amenazas. Los cibercriminales no suelen tener conocimiento alguno de la estructura interna de los sistemas de la organización que han tomado como objetivo. Por eso, la primera fase de un ataque suele ser la de reconocimiento. El ciberdelincuente inicia el ataque escaneando la red, para identificar los activos en búsqueda de vulnerabilidades conocidas, a través de las cuales ganar privilegios y obtener acceso a los activos más valiosos. El SOC debe conocer los servicios están ejecutándose en cualquier activo para poder medir la peligrosidad de un ataque, lanzar un exploit de Windows en un equipo mac no supone un peligro.

Para saber priorizar los recursos, se han de definir la importancia de los activos dentro de la organización, las consecuencias de que sufrieran un ataque y la importancia de la información que contienen. Por ello antes de la implantación de un SOC, para conocer los activos principales a defender se han de contestar a estas cuestiones:

- ¿Cuáles son los sistemas críticos para el funcionamiento de la empresa? ¿Qué sistemas son imprescindibles para la continuidad de negocio?, de forma que, si sufrieran un ataque la organización se vería bloqueada, estos son los activos más importantes a proteger.
- ¿Cuáles son los sistemas críticos para el funcionamiento diario? ¿Qué sistemas si cayeran no permitirían continuar con la operativa normal?, de forma que, aunque la organización pudiera seguir funcionando si cayeran no sería posible continuar con las tareas normales.
- ¿Cuáles son los sistemas de los que dependen los sistemas critico? ¿Qué sistemas en caso de fallo provocarían el fallo de algún sistema crítico?
- ¿Dónde se almacena la información sensible de la organización?

Respondiendo a estas preguntas se podrían clasificar los activos de la organización para poder priorizar los recursos del SOC

3.2.1 Métodos de descubrimiento de activos

Es muy complicado conocer con precisión los activos de la organización y los servicios que corren en ellos. El departamento de TI debería de tener un inventario de todo, de forma que podría tener una razonablemente precisa imagen. No obstante, es difícil mantener esta lista actualizada, lo usuarios pueden instalar software, se pueden descatalogar equipos o conectar equipos nuevos sin informar al departamento de IT. Por eso una herramienta de reconocimiento automático puede ser una solución al problema, para mantener el listado actualizado y adaptarlo a los posibles cambios en la organización de forma que el SOC siempre este actualizado.

Se puede realizar el reconocimiento automático siguiendo tres enfoques. Se pueden utilizar estas técnicas de forma individual o combinada. Cada uno de los enfoques necesita recursos y acceso diferentes, y pueden ser útiles para realizar un inventario más completo, por ejemplo, el inventario basado en host no identifica los equipos conectados a la red sin el agente instalado, pero eso se puede utilizar combinándolo con otro enfoque que detecte los nuevos hosts.

3.2.1.1 Monitorización pasiva de red

Se monitoriza los paquetes de la red de forma pasiva, con la información obtenida se identifican los hosts, los paquetes de software instalados, identificando los puertos y los protocolos. Por ejemplo, mediante la captura de tráfico en pcap y extrayendo los hosts presentes en las capturas de tráfico. Por ejemplo, con la herramienta NetworkMiner, es posible enumerar los hosts presentes en el tráfico almacenado en un pcap, además de mucha más información.

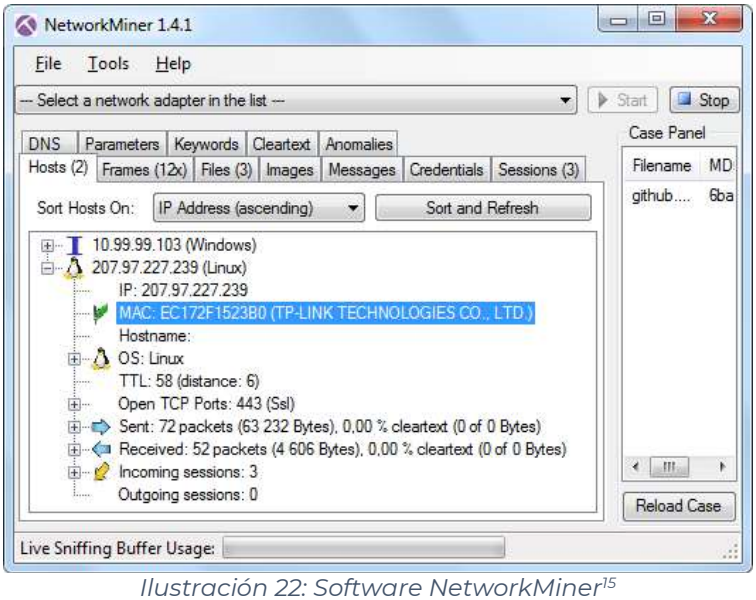


Ilustración 22: Software NetworkMiner[15]

[15] https://www.netresec.com/?page=networkminer

3.2.1 Escaneo activo de red

Se realiza una monitorización activa de la red, forzando a los hosts a contestar, la herramienta de monitorización basándose en la respuesta identifica la máquina, el software instalado y los puertos activos. Permite mantener un inventario de los hots, Servidores y demás dispositivos presentes en la red, de forma automática y actualizada, a cambio de generar más tráfico y ruido en la red, es posible que existan equipos que por medidas de seguridad no contesten a las peticiones, no pudiendo ser inventariados por este tipo de herramientas. Por ejemplo la herramienta WOCU monitoring, permite entre otras cosas el inventario activo de hosts.

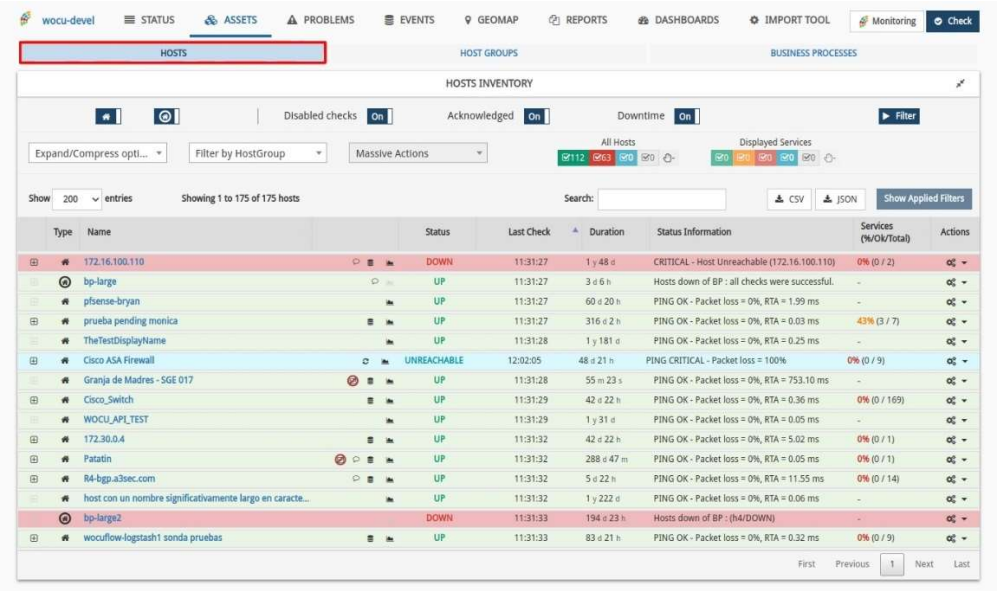


Ilustración 23: Inventario activo de dispositivos WOCU monitoring[16]

3.2.2 Inventario de software basado en host

Para realizar el inventario se instala un agente en los hosts que puede enumerar todo el software instalado en la máquina, no solo el activo en la red, o el que tiene un puerto a la escucha. Este enfoque da como resultado un listado mucho más preciso y profundo. Además, este tipo de herramientas tienen funciones forenses, ya que permiten detectar modificaciones en los equipos, como archivos borrados o modificados, cambios en los registros.

[16] https://docs.wocu-monitoring.com/index.html

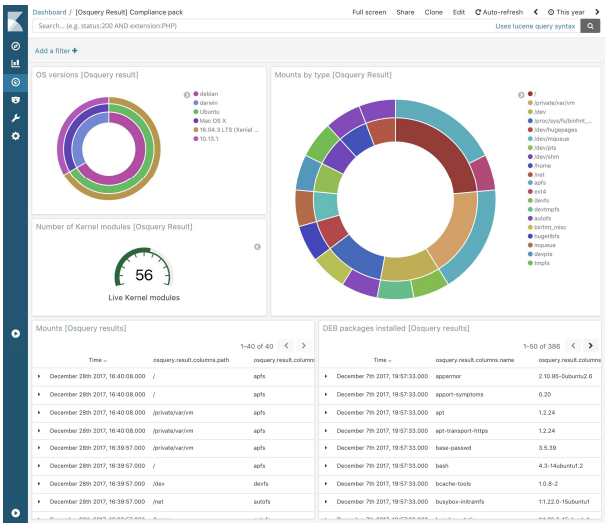


Ilustración 24: Resultados de osquery mostrados en kibana[17]

3.2.3 Entendiendo donde están los datos.

Para asegurar la confidencialidad, integridad y disponibilidad de los datos, se ha de controlar donde están almacenados, muchas organizaciones saben dónde están sus activos físicos, pero no dónde están sus datos, y no se puede proteger lo que no se conoce. Si la organización ha entregado sus datos a un proveedor en la nube, es fácil perder la noción de donde se encuentran. Y esto se convierte en un desafío cuanto más cambie la organización. Los días de tener todos sus datos residiendo en centros de datos que controlas están llegando a su fin. Hoy en día los datos de la organización se pueden encontrar en estas localizaciones:

- Físicamente en la organización. Centros de datos, equipos de oficina etc.
- Físicamente fuera de la organización. Discos duros extraíbles, memorias usb, unidades de copia de seguridad externas etc.
- Híbrido y en la nube. Almacenados en servidores de la organización y en la nube.
- En la nube. Los datos se almacenan en servidores en la nube.

Cuando los datos son almacenados en una nube o un sistema hibrido, la complejidad de realizar un seguimiento aumenta. Ya que la seguridad de los datos recae en el proveedor de la nube y escapa al control de la organización.

El SOC debe de ser consciente de donde se encuentran los datos más sensibles, y asegurar su confidencialidad, integridad y disponibilidad, monitorizando también los sistemas en la nube donde se encuentren, además de establecer políticas de copia de seguridad y de continuidad de negocio en caso de un incidente.

[17] https://osquery.io https://www.elastic.co/es/kibana

3.3 Activos a proteger en nuestra organización.

En la fase inicial de la implantación de nuestro SOC, únicamente se va a monitorizar y controlar la red interna de la empresa y los datos almacenados en los equipos conectados a esta. En esta fase se confía en los proveedores de nube externos y sus medidas de seguridad para mantener la confidencialidad, integridad y disponibilidad de los datos que almacenan. Con lo cual nos centraremos en los activos locales únicamente para definir los activos a proteger y su prioridad, para responder a las preguntas planteadas en el apartado 3.2. Igual que la estructura de red era un ejemplo, por motivos de confidencialidad, el estudio de los activos a proteger también lo es.

3.3.1 ¿Cuáles son los sistemas críticos para el funcionamiento de la empresa?

Como operadora de telefonía móvil para equipos de emergencia e IoT, los sistemas críticos no se encuentran en la red de la empresa, están en servidores externos y como se ha comentado en esta fase estos sistemas quedan fuera del SOC.

3.3.2 ¿Cuáles son los sistemas críticos para el funcionamiento diario?

La empresa trabaja con software en la nube, tanto el erp, el software de gestión y facturación, y los documentos ofimáticos están en la nube. Fue una decisión tomada después de un incidente de seguridad, de forma que mientras los proveedores de dichos servicios sigan operando, aunque los equipos de la oficina se vieran comprometidos, se podría teletrabajar o operar desde una localización diferente. Hay que mantener una política de cambio de claves periódico y utilizar un segundo factor de autenticación, por si en caso de robo de credenciales tuviera el menor impacto posible.

3.3.3 ¿Cuáles son los sistemas de los que dependen los sistemas critico?

En el proceso de montaje y fabricación de los equipos se utiliza un software de programación y verificación, este software se almacena en el servidor de fabricación, si este equipo se viera comprometido dificultaría el proceso de fabricación. Hay que realizar copias de seguridad de la base de datos y crear un plan de contingencia que en caso de fallo permitiera continuar con la fabricación sin problemas.

La atención al cliente utiliza un servidor, si este se viera comprometido no se podría dar servicio a los clientes, ni solventar incidencias, además de almacenar numerosa información técnica. También tiene que estar este servidor en el plan de copias de seguridad y disponer de un servidor backup que poder activar en caso de que este fallara para poder continuar con el servicio al cliente.

3.3.4 ¿Dónde se almacena la información sensible de la organización?

Aunque la información más sensible se almacena en la nube, en el servidor de copias de seguridad se almacena información importante de la organización, y se realiza copias de seguridad de los equipos y los documentos. De toda esta información se hacen copias de seguridad redundantes en la nube. Es un activo que hay que monitorizar y controlar el acceso.

En el servidor de desarrollo se ejecutan los procesos en pruebas y se encuentra el repositorio de código, se almacena información industrial importante para la empresa, se ha de proteger y vigilar.

Además de la información técnica presente en los servidores de fabricación y servicio técnico posen mucha información para uso exclusivo de la organización.

3.4 Descubrimiento de activos en nuestra organización.

La red de mi organización es pequeña, y está bastante controlada, no suelen entrar equipos nuevos sin que se sepa en el SOC, a pesar de tener los activos de la red controlados, para evitar la presencia de activos ocultos o por lo menos no controlados, se va a realizar periódicamente reconocimientos de los hosts presentes, mediante el escaneo pasivo de la red y mediante software basado en host.

3.4.1 Descubrimiento mediante escaneo pasivo de la red.

El servidor de Security Onion del SOC está conectado directamente al firewall de cabecera y está esnifando todo el tráfico de la organización, este tráfico es almacenado en el servidor para posteriores tareas de forense, El dashboard de del servidor permite la desca de esos paquetes en formato pcap mediante unos criterios de búsqueda.

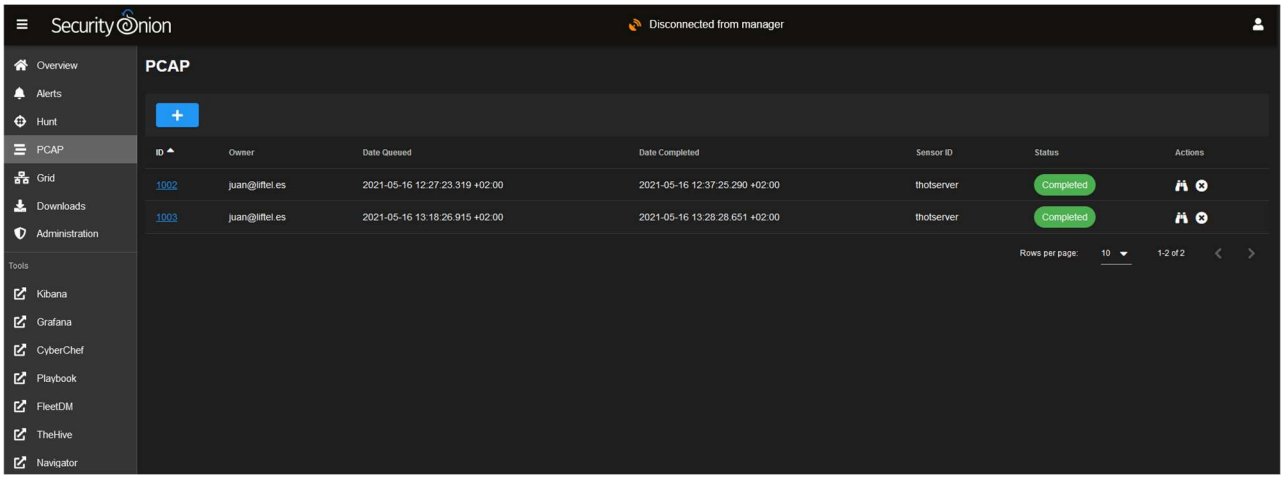


Ilustración 25: Dashboard para la descarga de los ficheros pcap

Periódicamente nos descargaremos los ficheros pcap del tráfico almacenado y lo analizaremos mediante NetworkMiner, listando los hosts que han enviado tramas y comprobando si están todos en el listado de host de la organización, o si hay alguno nuevo o sospechoso.

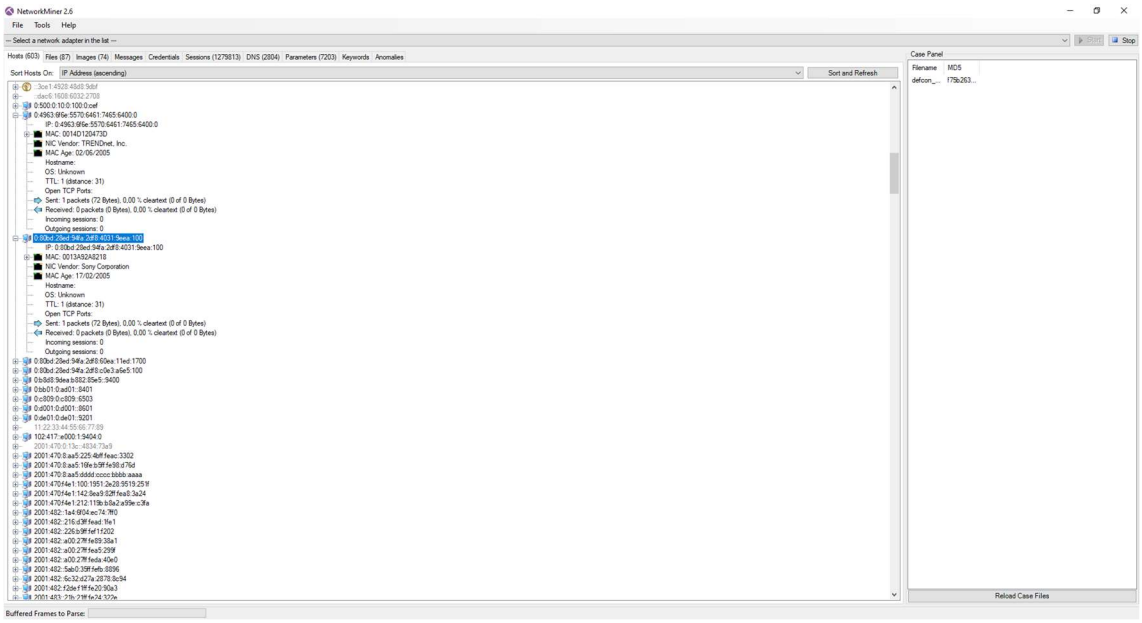


Ilustración 26: Listado de hosts en un pcap con NetworkMiner

3.4.2 Inventario de software basado en host.

Otra de las útiles herramientas que incorpora Security Onion son Osquery y Fleet.

3.4.2.1 Osquery

Osquery instala un useragent en los hosts y permite mediante el lenguaje sql realizar consultas de toda la información del host, como registros, extensiones de Chrome o certificados instalados.

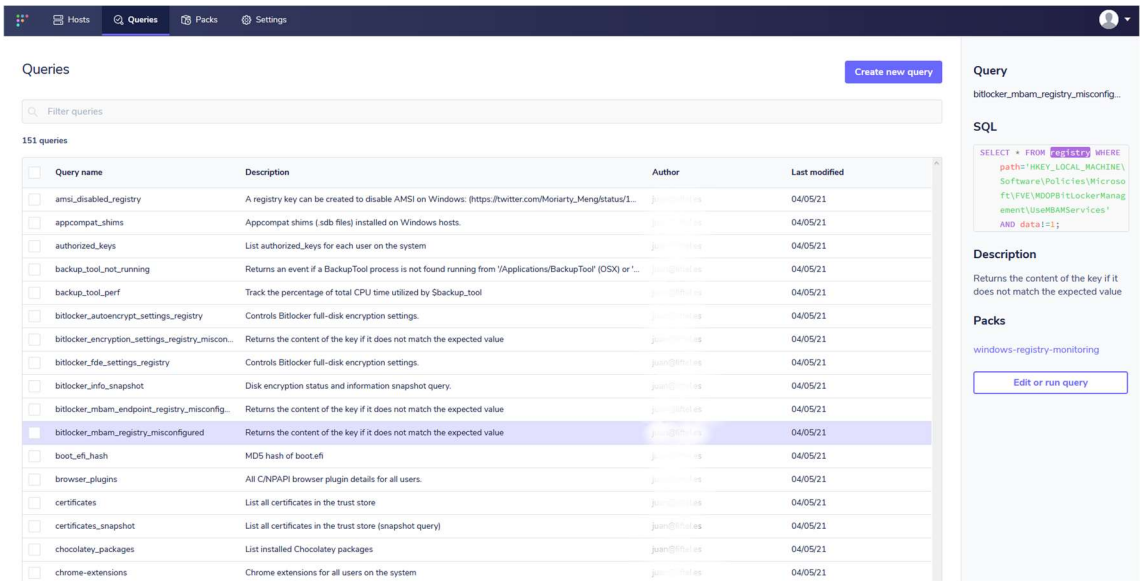


Ilustración 27: Listado de scripts

Osquery permite la creación de packs, que son un conjunto establecido de querys, por ejemplo, para inspeccionar el registro de Windows o conocer todo el software instalado.

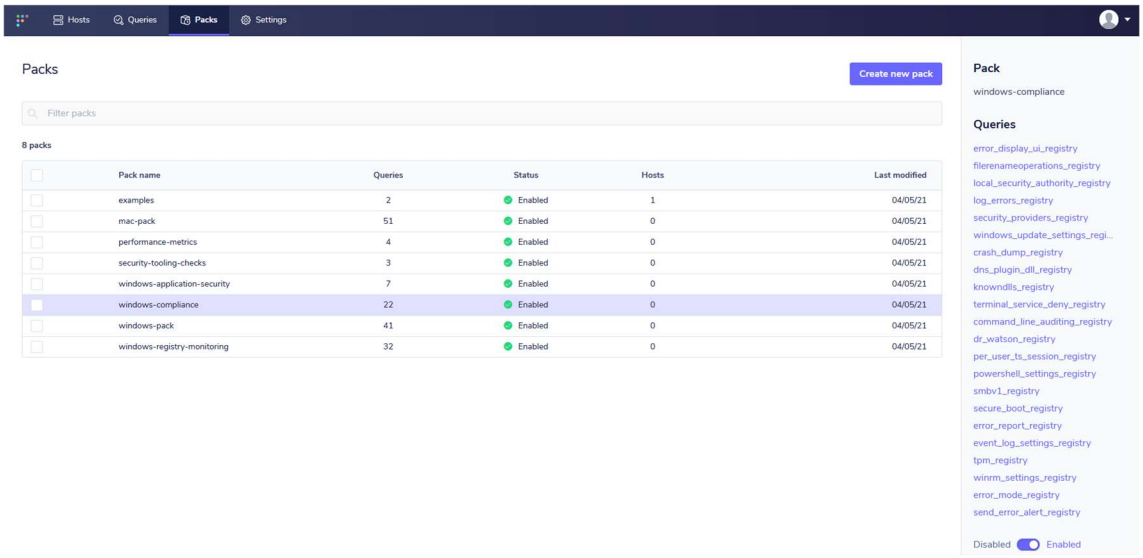


Ilustración 28: Ejemplos de packs de Osquery

3.4.2.1 Fleet

Fleet[18] es un manager de osquery, permite visualizar todos los hosts, gestionar las querys y ver el resultado, además de enviar los logs, dispone un api a través de la cual los endpoints envían la información y puede ser consultada. Es aquí donde periódicamente lanzaremos query del estado de los hosts para compararlas con los resultados obtenidos anteriormente y poder comprobar si existe algún cambio en el software de los hosts.

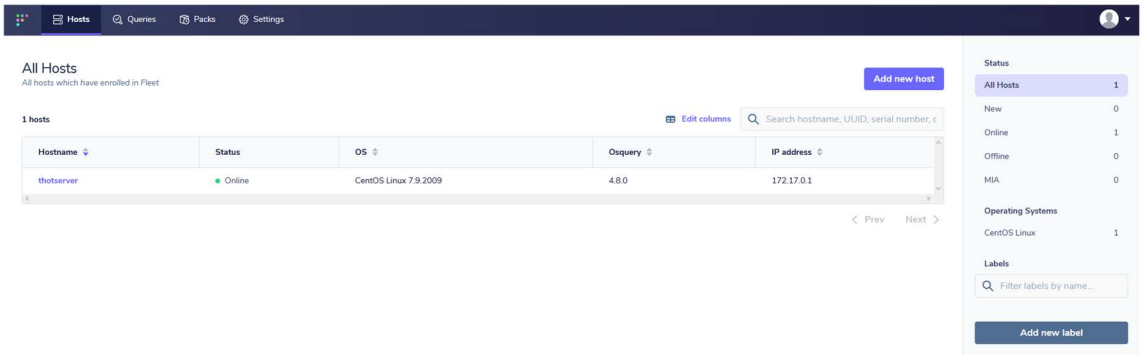


Ilustración 29: Aspecto del portal de Fleet

[18] https://fleetdm.com/

4. Detección de los activos vulnerables

El siguiente paso para la implementación del SOC, una vez conocidos los activos de la organización es conocer sus debilidades, siempre hay que seguir la máxima, “No se puede proteger lo que no se conoce”. Conocer cómo es posible atacar nuestra organización para en caso de un incidente de seguridad es transcendental para determinar donde se destinan los recursos.

Es muy importante conocer, conocer que activos son más vulnerables para reforzar alrededor de ellos, y de los sistemas de los que dependen, los recursos de securización. Se puede dar el caso que para ciertos procesos de la organización se tenga que seguir utilizando un equipo desactualizado, o se tiene que utilizar un software en una versión con vulnerabilidades conocidas, esto podría ser un punto de exposición importante, poniendo en riesgo el resto de equipos de la red, si se conoce se pueden tomar medidas extra para minimizar los posibles efecto de un ataque, incluso herramientas para en caso de ataque aislarlos de la red o aumentar los recursos de su protección.

Aunque se pretenda no siempre es posible solucionar todas las vulnerabilidades de los sistemas, puede que no exista un parche para esa versión de software o simplemente no es posible solucionarla porque el fallo se encuentra en el núcleo del programa y no es posible parchearlo, o la vulnerabilidad está en el firmware de un equipo y simplemente no se puede reprogramar. Por ello es importante conocer la repercusión de que estas vulnerabilidades sean explotadas, para prevenirlos, y tener un plan de respuesta en caso de incidente de seguridad.

Por definición no existe el software totalmente seguro todo el tiempo. El software presente a nuestro alrededor, ya sean los sistemas operativos, el que corre en servidores, el de nuestro móvil o el firmware de nuestra tele es por defecto vulnerable. ¿Quién no ha visto un error de Windows en una pantalla del aeropuerto o en una estación de tren?, incluso los patinetes eléctricos que pueden ser controlados por bluetooth, un ejemplo muy comentado actualmente es el de un cinturón de castidad conectado con fallos en el api, que permite a un atacante pedir rescates a usuarios a cambio de no bloquearlo permanentemente. El código de los programas puede tener fallos potencialmente explotables, una liberación incorrecta de memoria, una entrada de datos que no controla el formato, o incluso el uso de una librería vulnerable. Principalmente esto es culpa de que durante la implementación no se tiene en cuenta la seguridad por defecto, normalmente se programa el código y después se protege, en lugar de pensar ya en la seguridad durante la programación. Aunque si se programara con la seguridad por defecto, los atacantes son creativos siempre están desarrollando nuevos métodos de ataque, un programa seguro hoy puede dejar de serlo dentro de un año. Por eso el análisis de vulnerabilidades es un proceso continuo que debe estar siempre actualizado, aun así, es una tarea compleja para intentar automatizarla, debido a que para entender la forma en que se ataca una vulnerabilidad hay que entender profundamente cómo funciona el programa, lo que se suele utilizar son escáneres de vulnerabilidades, que son programas con una gran base de datos de vulnerabilidades de software conocidos y realiza un escaneo buscando dichas vulnerabilidades.

Ilustración 30: Cinturón de castidad inteligente, con una vulnerabilidad explotada por ciberdelincuentes para pedir rescates a cambio de no bloquearlos.[19]

4.1 Escáner de vulnerabilidades

Un escáner de vulnerabilidades es una herramienta para analizar los servicios y los equipos de una red en busca de vulnerabilidades y amenazas conocidas. Para profundizando en el funcionamiento de un escáner de vulnerabilidades, hay que entender en que consiste el análisis de vulnerabilidades. El análisis de vulnerabilidades es el proceso de identificar los sistemas en la red que tiene vulnerabilidades conocidas, tales como exploits conocidos, Puntos de acceso inseguros, errores de programación aprovechables o errores de configuración que pueden ser utilizados por un atacante. Esta es la razón por la cual el análisis de vulnerabilidades en nuestros entornos de red simplemente trata de identificar los paquetes de software que contienen vulnerabilidades conocidas.

4.1.1 Tipos de escáner de vulnerabilidades.

Existen diferentes tipos de escáneres según el tipo de vulnerabilidades que auditan.

- Basados en host: Escanea un host o sistema, se ejecutan en el sistema objetivo rastreando los eventos e informando del análisis de seguridad.
- Basados en red: Escanea los equipos de una red, detectando sistemas operativos, los puertos abiertos e identifican servicios que se ejecutan en esos puertos, revelando posibles vulnerabilidades asociados a estos servicios.
- Basados en web: Escanean aplicaciones web en busca de vulnerabilidades (sql injection, script injection, Cross-Site Scripting (XSS)).

[19]https://www.genbeta.com/actualidad/hacker-ha-logrado-hacerse-control-este-cinturon-castidad-conectado-pide-bitcoins-a-victimas-para-desbloquearlo

- Basados en base de datos: Escanean bases de datos detectando inseguridades, utilizando herramientas y técnicas para evitar vulnerabilidades.

Normalmente se utiliza una combinación de escáneres para cubrir todo el espectro de vulnerabilidades, host, red, portales web de la organización.

4.1.2 Escáneres presentes en el mercado

En el mercado existen múltiples marcas y tipos de escáneres, comerciales y open source como, por ejemplo:

- AlienVault USM: Es una solución pensada para empresas, está disponible como SaaS, no requiere instalación, realiza el escaneo de vulnerabilidades de la red, también tiene funciones de descubrimiento de activos, monitoreo del comportamiento, detección de intrusiones, eventos y administración de registros.
- InsightVM: Es un escáner de la empresa rapid7, se vende bajo licencia, puede recopilar, monitorear y analizar el riesgo de redes nuevas y existentes.
- Intruso: Es un escáner de vulnerabilidades proactivo que realiza escaneos cada vez que se descubren nuevas vulnerabilidades, detecta más de 10,000 debilidades de seguridad, ayudando a reducir su superficie de ataque al resaltar los puertos y servicios que no deben estar expuestos a Internet. Es popular entre las pymes porque facilita la gestión de vulnerabilidades para equipos pequeños.
- Acunetix: Es un escáner comercial que escanea el perímetro de la red para detectar más de 50,000 vulnerabilidades conocidas y configuraciones incorrectas, incorpora el escáner OpenVAS para proporcionar un escaneo de seguridad de red completo.
- OpenVAS: Es seguramente el escáner de vulnerabilidades open source más popular, incluye muchos servicios y herramientas y lo hace perfecto para pruebas de vulnerabilidad de red. Nació en 2005 como un fork de Nessus cuando los desarrolladores decidieron abandonar el proyecto open source y convertirlo en un escáner comercial.
- Nessus: Es un escáner de vulnerabilidades de Tenable, utilizado por millones de personas, escanea diferentes tipos de activos; Sistema operativo, Hipervisores, Dispositivos de red, base de datos, Servidores web, cortafuegos. Debido a su versatilidad y rapidez es uno de los escáneres más populares del mercado.
- Nmap: No es un escáner de vulnerabilidades propiamente dicho, es un escáner de puertos, pero dispone de la función NSE que permite la ejecución de scripts automatizando el proceso de detección de vulnerabilidades. Es un proyecto open source

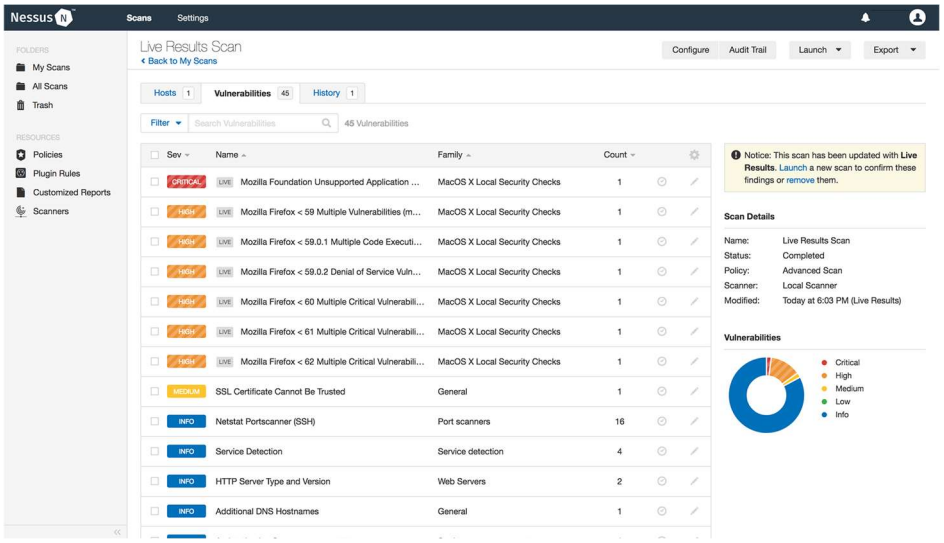


Ilustración 31: Resultado de un escaneo con Nessus

La mayoría de los escáneres en el mercado, y los mejores, son comerciales, no hay muchos proyectos open source, y aun menos que den una buena relación entre positivos y falsos negativos, OpenVas es quizás el mejor de los open source y queda mal parado en su comparación con Nessus, con quien comparte su origen. Supongo que esto es porque se necesitan muchos recursos para mantener actualizada la base de datos y realizar un motor de escaneo que tenga la suficiente profundidad en los activos para detectar las vulnerabilidades.

4.1.3 Automatizar el análisis de vulnerabilidades

Para automatizar el Análisis de Vulnerabilidades se pueden utilizar dos enfoques.

4.1.3.1 Escaneo activo de red

El escaneo activo de red consiste en generar tráfico diseñado para provocar una respuesta en los hosts. Conociendo el tráfico generado se analiza la respuesta en un motor de análisis que da como resultado la configuración del host y la identificación de los servicios que están expuestos. El resultado de este análisis se cruza con una base de datos actualizada de vulnerabilidades, elaborando una lista de vulnerabilidades conocidas existentes en los activos de red.

4.1.3.2 Análisis basado en host

Mediante un agente instalado en el host, el motor de análisis puede realizar un escaneo más preciso y exhaustivo de vulnerabilidades, al inspeccionar el software presente en el host, no solamente el que tiene un puerto expuesto, y comparándolo con una base de datos de paquetes de software con vulnerabilidades conocidas elaborar una lista de activos vulnerables.

4.1.3.3 Enfoques

Estos dos enfoques se pueden combinar, como por ejemplo utilizar OpenVas para el escaneo activo de red y forticlient como agente en los hosts. Ambos enfoques dependen para la detección de una base de datos de vulnerabilidades conocidas, se han de actualizar frecuentemente y realizar un escaneo con cada actualización, además de cada vez que se detecta un nuevo activo o servicio en la red, mediante los métodos de descubrimiento de activos. Múltiples agencias (CVE, INCIBE, NVD etc.) publican periódicamente las vulnerabilidades reportadas, se ha de mantener actualizada la base de datos con estas nuevas publicaciones para asegurar una detección fiable.

4.1.4 Cuestiones a contestar

Por lo tanto, para conocer las debilidades de los activos de la red, en el SOC se han de contestar a estas cuestiones:

- ¿Qué configuración tienen los activos de la red?, están configurados por defecto, o tienen una configuración segura.
- ¿Qué exposición tienen? Como de expuestos están los diferentes activos, para entender su potencial vulnerabilidad,
- ¿Existen activos con vulnerabilidades conocidas?

4.2 Detección de activos vulnerables en nuestra organización

Para contestar a las preguntas planteadas en el apartado anterior, dentro de la planificación de tareas del SOC, se escaneará la red en busca de posibles vulnerabilidades de forma periódica cada mes, y cuando se introduzca un equipo nuevo en la red.

La distribución de auditoría de redes instalada en el servidor de nuestro SOC, no dispone de un escáner de vulnerabilidades instalado, pero como mencionamos en el apartado 2.8.3 Security Onion es fácilmente ampliable mediante Docker[20]. Utilizamos el escáner de vulnerabilidades Seccubus[21] ejecutándose en un Docker.

Seccubus es una herramienta que permitir ejecutar de manera automatizada una gran cantidad de herramientas para el escaneo de vulnerabilidades, tales como Nessus, OpenVAS, Nmap o OWASP ZAP. Facilita la automatización de escaneos de vulnerabilidades con periodos programados, y compara los resultados del escaneo de cada herramienta con los resultados de escaneos anteriores, informando de los cambios, ayudando al analista en el análisis rápido de sus resultados, tanto en el primer escaneo como en los escaneos repetidos. Los informes de cambio de los escaneos repetidos, avalan los hallazgos que el analista solo debe considerar cuando aparecen por primera vez o cuando cambia el resultado.

[20] https://www.docker.com/
[21] https://www.seccubus.com/

Uno de los mayores inconvenientes de escaners como OpenVas o Nessus es que a pesar de ser herramientas muy valiosas también generan mucho ruido durante los escaneos. A menudo invierten más del doble de tiempo en realizar un escaneo que el tiempo que realmente es necesario para realizarlo. Frank Breedijk creo Seccubus para analizar más eficazmente los resultados ofrecidos por los escáneres más utilizados. Se pensó para ser utilizado por equipos encargados de la seguridad informática de organizaciones, que como tarea regularmente tienen que escanear la red de su organización.

Para que Seccubus pueda utilizar los resultados de los diferentes escáneres estos se han de normalizar, una vez se obtiene el resultado del escaneo se convierten en formato IVIL, de forma que sea compatible con Seccubus.

Seccubus actualmente trabaja con los siguientes escáneres:

- Nessus
- OpenVAS
- Nmap
- Nikto
- Medusa
- SSLyze
- Qualys SSL labs
- Testssl.sh
- SkipFish
- Zap

4.2.1 Uso de Seccubus.

Ejecutaremos Seccubus con un contenedor Docker, simplemente con el comando run, se descargará el contenedor de Docker hub[22].

```
[cerocold@thotserver ~]$ sudo docker run -it seccubus/seccubus /bin/bash
[sudo] password for cerocold:
Unable to find image 'seccubus/seccubus:latest' locally
latest: Pulling from seccubus/seccubus
c8773622led0: Pull complete
c6a586c916d6: Pull complete
```

Ilustración 32: Ejecución del contenedor de seccubus

Una vez ejecutado, en el navegador web accedemos a la dirección ip del contenedor y nos pide usuario y contraseña, las credenciales por defecto son user: admin password: *GiveMeVulns!*

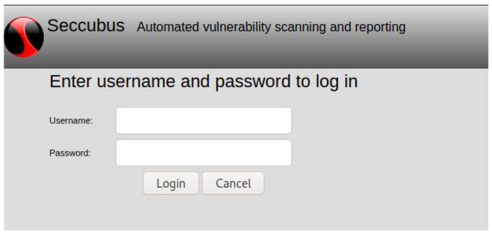


Ilustración 33: Panel de login de Seccubus

[22] https://hub.docker.com/

Una vez logueados crearemos un workspace y después dentro del definiremos las tareas de los escáneres que queremos realizar.

Ilustración 34: Escaneres del workspace

Al crear las tareas de los escáneres, tendremos que definir el tipo de escáner, los parámetros que queremos pasarle en la llamada y el equipo o equipos a escanear.

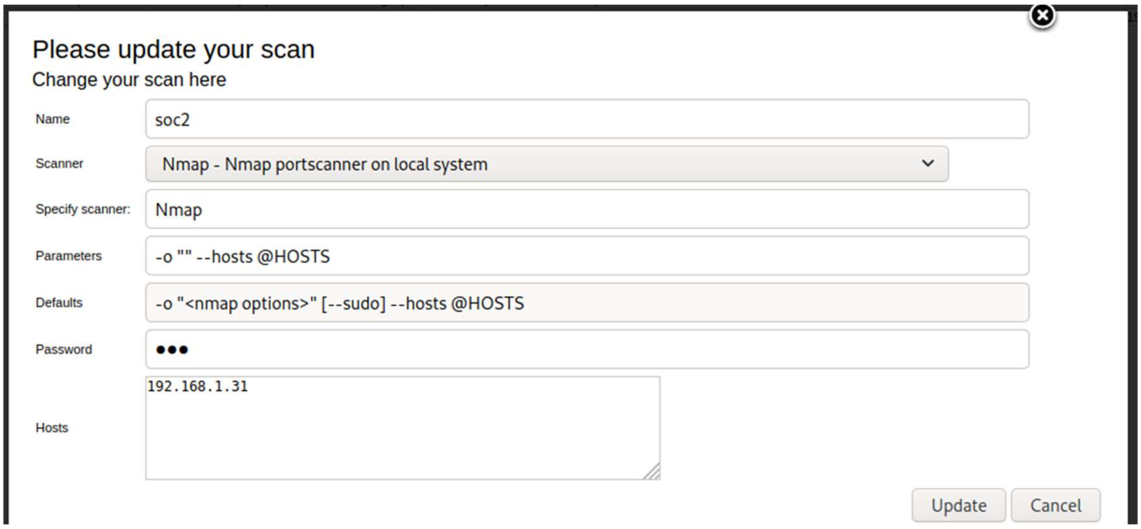


Ilustración 35: Definición de un escaner con Nmap

Cuando tenemos creado el workspace y definidos los escáneres, volvemos al termina y en la línea de comando del contenedor ejecutamos el escáner del workspace que queremos. Una vez terminado el escaner mostrará la información en la web.

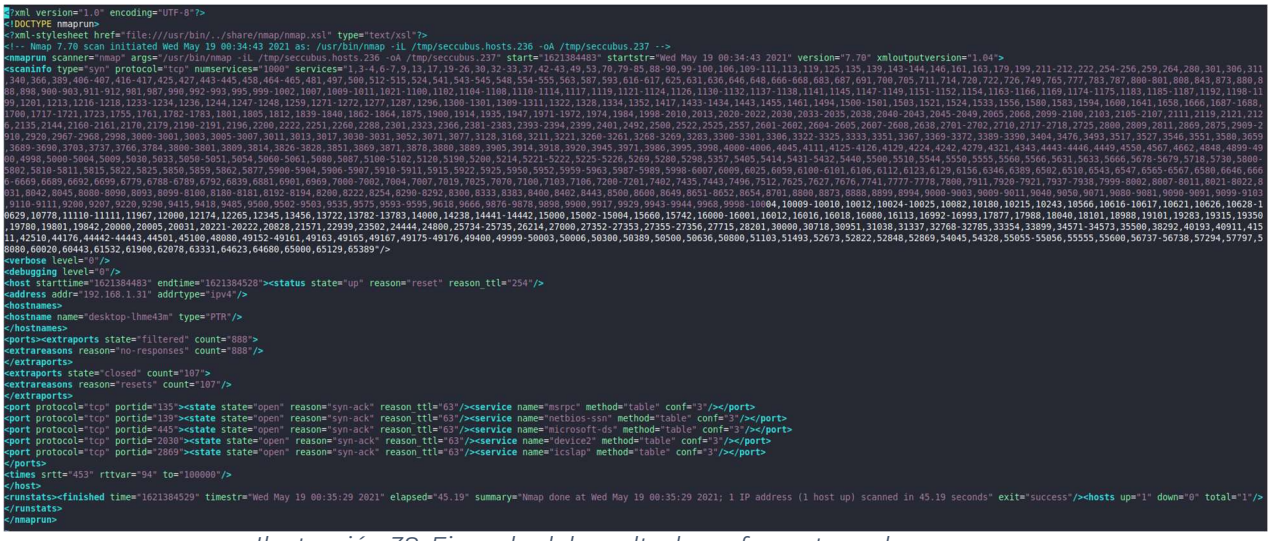
```
bash-4.4# do-scan --workspace tfm --scan soc2
Starting scan 'soc2' from workspace 'tfm'
Sending notifications for scan start...
0 notification(s) sent
cmd: /opt/seccubus/scanners/Nmap/scan --workspace 'tfm' --scan 'soc2' -o "" --hosts /tmp/seccubus.hosts.236
Executing /usr/bin/nmap -iL /tmp/seccubus.hosts.236 -oA '/tmp/seccubus.237'
Scanning done, converting .xml to ivil
Use of uninitialized value in join or string at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1301.
Use of uninitialized value $key in hash element at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1307.
Use of uninitialized value in join or string at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1301.
Use of uninitialized value $key in hash element at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1307.
Use of uninitialized value in join or string at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1301.
Use of uninitialized value $key in hash element at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1307.
Use of uninitialized value in join or string at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1301.
Use of uninitialized value $key in hash element at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1307.
Use of uninitialized value in join or string at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1301.
Use of uninitialized value $key in hash element at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1307.
Use of uninitialized value in join or string at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1301.
Use of uninitialized value $key in hash element at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1307.
Use of uninitialized value in join or string at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1301.
Use of uninitialized value $key in hash element at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1307.
Importing ivil
Use of uninitialized value in join or string at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1301.
Use of uninitialized value $key in hash element at /usr/share/perl5/vendor_perl/XML/Simple.pm line 1307.
Sending notifications for scan end...
0 notification(s) sent

Done
```

Ilustración 36: Ejecución de un escaner de nmap

Los resultados se presentan en diferentes formatos, para que sea más fácil procesarlos y compararlos con escaneos anteriores y poder encontrar diferencias.

Ilustración 37: Resultados del escaneo

Aquí se puede ver por ejemplo el resultado en formato xml del escaneo realizado.



```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl" type="text/xsl"?>
<!-- Nmap 7.70 scan initiated Wed May 19 00:34:43 2021 as: /usr/bin/nmap -iL /tmp/seccubus.hosts.236 -oA /tmp/seccubus.237 -->
<nmaprun scanner="nmap" args="/usr/bin/nmap -iL /tmp/seccubus.hosts.236 -oA /tmp/seccubus.237" start="1621384483" startstr="Wed May 19 00:34:43 2021" version="7.70" xmloutputversion="1.04">
<scaninfo type="syn" protocol="tcp" numservices="1000" services="1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256,259,264,280,301,306,311
,340,366,389,406-407,416-417,425,427,443-445,458,464-465,481,497,500,512-515,524,541,543-545,548,554-555,563,587,593,616-617,625,631,636,646,648,666-668,683,687,691,700,705,711,714,720,722,726,749,765,777,783,787,800-801,808,843,873,880,8
88,898,900-903,911-912,981,987,990,992-993,995,999-1002,1007,1009-1011,1021-1100,1102,1104-1108,1110-1114,1117,1119,1121-1124,1126,1130-1132,1137-1138,1141,1145,1147-1149,1151-1152,1154,1163-1166,1169,1174-1175,1183,1185-1187,1192,1198-11
99,1201,1213,1216-1218,1233-1234,1236,1244,1247-1248,1259,1271-1272,1277,1287,1296,1300-1301,1309-1311,1322,1328,1334,1352,1417,1433-1434,1443,1455,1461,1494,1500-1501,1503,1521,1524,1533,1556,1580,1583,1594,1600,1641,1658,1666,1687-1688,
1700,1717-1721,1723,1755,1761,1782-1783,1801,1805,1812,1839-1840,1862-1864,1875,1900,1914,1935,1947,1971-1972,1974,1984,1998-2010,2013,2020-2022,2030,2033-2035,2038,2040-2043,2045-2049,2065,2068,2099-2100,2103,2105-2107,2111,2119,2121,212
9,2135,2144,2160-2161,2170,2179,2190-2191,2196,2200,2222,2251,2260,2288,2301,2323,2366,2381-2383,2393-2394,2399,2401,2492,2500,2522,2525,2557,2601-2602,2604-2605,2607-2608,2638,2701-2702,2710,2717-2718,2725,2800,2809,2811,2869,2875,2909-2
910,2920,2967-2968,2998,3000-3001,3003,3005-3007,3011,3013,3017,3030-3031,3052,3071,3077,3128,3168,3211,3221,3260-3261,3268-3269,3283,3300-3301,3306,3322-3325,3333,3351,3367,3369-3372,3389-3390,3404,3476,3493,3517,3527,3546,3551,3580,3659
,3689-3690,3703,3737,3766,3784,3800-3801,3809,3814,3826-3828,3851,3869,3871,3878,3880,3889,3905,3914,3918,3920,3945,3971,3986,3995,3998,4000-4006,4045,4111,4125-4126,4129,4224,4242,4279,4321,4343,4443-4446,4449,4550,4567,4662,4848,4899-49
00,4998,5000-5004,5009,5030,5033,5050-5051,5054,5060-5061,5080,5087,5100-5102,5120,5190,5200,5214,5221-5222,5225-5226,5269,5280,5298,5357,5405,5414,5431-5432,5440,5500,5510,5544,5550,5555,5560,5566,5631,5633,5666,5678-5679,5718,5730,5800-
5802,5810-5811,5815,5822,5825,5850,5859,5862,5877,5900-5904,5906-5907,5910-5911,5915,5922,5925,5950,5952,5959-5963,5987-5989,5998-6007,6009,6025,6059,6100-6101,6106,6112,6123,6129,6156,6346,6389,6502,6510,6543,6547,6565-6567,6580,6646,666
6-6669,6689,6692,6699,6779,6788-6789,6792,6839,6881,6901,6969,7000-7002,7004,7007,7019,7025,7070,7100,7103,7106,7200-7201,7402,7435,7443,7496,7512,7625,7627,7676,7741,7777-7778,7800,7911,7920-7921,7937-7938,7999-8002,8007-8011,8021-8022,8
031,8042,8045,8080-8090,8093,8099-8100,8180-8181,8192-8194,8200,8222,8254,8290-8292,8300,8333,8383,8400,8402,8443,8500,8600,8649,8651-8652,8654,8701,8800,8873,8888,8899,8994,9000-9003,9009-9011,9040,9050,9071,9080-9081,9090-9091,9099-9103
,9110-9111,9200,9207,9220,9290,9415,9418,9485,9500,9502-9503,9535,9575,9593-9595,9618,9666,9876-9878,9898,9900,9917,9929,9943-9944,9968,9998-10004,10009-10010,10012,10024-10025,10082,10180,10215,10243,10566,10616-10617,10621,10626,10628-1
0629,10778,11110-11111,11967,12000,12174,12265,12345,13456,13722,13782-13783,14000,14238,14441-14442,15000,15002-15004,15660,15742,16000-16001,16012,16016,16018,16080,16113,16992-16993,17877,17988,18040,18101,18988,19101,19283,19315,19350
,19780,19801,19842,20000,20005,20031,20221-20222,20828,21571,22939,23502,24444,24800,25734-25735,26214,27000,27352-27353,27355-27356,27715,28201,30000,30718,30951,31038,31337,32768-32785,33354,33899,34571-34573,35500,38292,40193,40911,415
11,42510,44176,44442-44443,44501,45100,48080,49152-49161,49163,49165,49167,49175-49176,49400,49999-50003,50006,50300,50389,50500,50636,50800,51103,51493,52673,52822,52848,52869,54045,54328,55055-55056,55555,55600,56737-56738,57294,57797,5
8080,60020,60443,61532,61900,62078,63331,64623,64680,65000,65129,65389"/>
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1621384483" endtime="1621384528"><status state="up" reason="reset" reason_ttl="254"/>
<address addr="192.168.1.31" addrtype="ipv4"/>
<hostnames>
<hostname name="desktop-lhme43m" type="PTR"/>
</hostnames>
<ports><extraports state="filtered" count="888">
<extrareasons reason="no-responses" count="888"/>
</extraports>
<extraports state="closed" count="107">
<extrareasons reason="resets" count="107"/>
</extraports>
<port protocol="tcp" portid="135"><state state="open" reason="syn-ack" reason_ttl="63"/><service name="msrpc" method="table" conf="3"/></port>
<port protocol="tcp" portid="139"><state state="open" reason="syn-ack" reason_ttl="63"/><service name="netbios-ssn" method="table" conf="3"/></port>
<port protocol="tcp" portid="445"><state state="open" reason="syn-ack" reason_ttl="63"/><service name="microsoft-ds" method="table" conf="3"/></port>
<port protocol="tcp" portid="2030"><state state="open" reason="syn-ack" reason_ttl="63"/><service name="device2" method="table" conf="3"/></port>
<port protocol="tcp" portid="2869"><state state="open" reason="syn-ack" reason_ttl="63"/><service name="icslap" method="table" conf="3"/></port>
</ports>
<times srtt="453" rttvar="94" to="100000"/>
</host>
<runstats><finished time="1621384529" timestr="Wed May 19 00:35:29 2021" elapsed="45.19" summary="Nmap done at Wed May 19 00:35:29 2021; 1 IP address (1 host up) scanned in 45.19 seconds" exit="success"/><hosts up="1" down="0" total="1"/>
</runstats>
</nmaprun>
```


Ilustración 38: Ejemplo del resultado en formato xml

5. Identificación de las amenazas

Internet no se diseñó pensando en que fuera segura, nunca se pensó que llegará a convertirse en lo que es actualmente. A día de hoy todo el mundo lo sepa o no seguramente haya sido atacado. Internet es una red global, no hay distancias, un atacante puede encontrar una víctima en cualquier parte del mundo desde cualquier parte del mundo, tiene toda la red a su alcance. Que no exista un coste para llegar desde el atacante a la víctima hace que le cueste lo mismo atacar a cualquiera, si a eso se le suma que todo el proceso de escaneo se puede automatizar, un atacante cualquiera puede dedicarse a escanear la red buscando objetivos con una vulnerabilidad específica que atacar, no tiene por qué saber a quién ataca únicamente que sea vulnerable. Todos los equipos conectados a internet están constantemente atacados, únicamente es necesario una vulnerabilidad no solucionada para que el ataque tenga éxito.

En el apartado anterior se trató el nivel de detección de activos vulnerables, el nivel de detección de brechas de seguridad, supone profundizar en este campo, la identificación de amenazas es la forma de detectar los ataques que están dirigidos a explotar los activos vulnerables. Hay ataques que tienen como objetivo explotar vulnerabilidades concretas con metodologías conocidas o con el uso de ficheros identificados; este tipo de ataque mediante el uso de firmas se pueden detectar fácilmente. Sin embargo, existen ataques menos conocidos, en estos casos se ha de intentar detectarlos mediante el análisis de eventos y anomalías que puedan identificar las técnicas utilizadas.

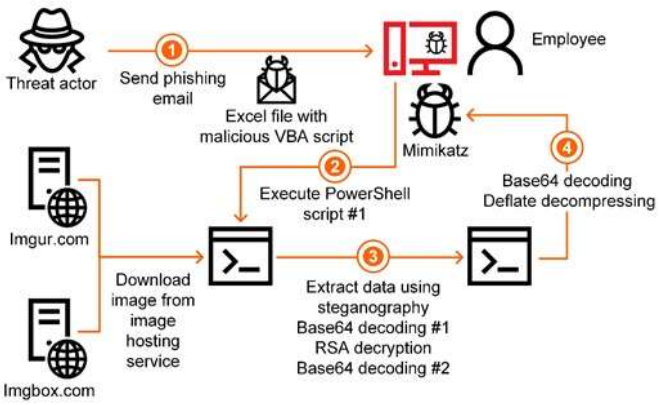


Ilustración 39: Esquema de un ataque para la obtención de credenciales[23]

Normalmente la primera fase de un ataque es la fase de descubrimiento para identificar los activos de la red y detectar si alguno es vulnerable. Localizar tráfico desde un activo de la red que tiene como objetivo escanear la red de la organización, puede ser un indicio de un ataque y es esencial para evaluar si realmente es un ataque desde ese host Para poder detectar las amenazas desconocidas hay que ser capaz de detectar el ruido y los indicios de comportamiento anómalos. Por ende, para detectar estas amenazas se han

[23] https://haycanal.com/noticias/14624/la-sofisticacion-de-los-ciberataques-dirigidos-al-sector-industrial

de tener metodologías flexibles, los ataques son diseñados para evadir los diferentes mecanismos de detección de amenazas conocidos y cambian rápidamente. Los sistemas de identificación de amenazas deben de ser capaces de cambiar a la misma velocidad.

La estructura de red y donde se implementan los sistemas de identificación de las amenazas es un tema importante, la forma de trabajo ha cambiado, este es el principal motivo por el que se realiza este trabajo de fin de master, los empleados utilizan sus dispositivos desde su casa teletrabajando o en movilidad, los sistemas de protección internos al perímetro de red de la organización no son válidas cuando el trabajador esta fuera de la red. Si un dispositivo se ha visto comprometido estando fuera de los sistemas de seguridad de la organización, cuando se conecte a la red podría ser la puerta para un ataque. Estas nuevas circunstancias deben ser tenidas en cuenta en la implementación de los sistemas de identificación de amenazas.

Se ha de implementar un sistema de identificación de amenazas adecuado que pueda dar respuesta a las siguientes preguntas:

- ¿Mi organización está recibiendo amenazas?
- ¿Qué técnicas se están utilizando en los ataques?
- ¿Cuál es el origen de los ataques?

5.1 Detección de anomalías

Pero ¿Cómo saber que es anómalo si no se tiene una base sólida del comportamiento normal? Es necesario que el SOC conozco lo que es el comportamiento normal de la red, debe tener una sólida referencia de lo que se considera normal, ya que muchas veces los ataques no generan un comportamiento que haga saltar las alarmas, los atacantes se ocupan de ello.

Saber que patrones son normales es como tener un modelo, un modelo con el que poder comparar estados o condiciones, y sobre el que poder tomar mediciones. Se ha de recoger, captura y definir modelos de comportamiento normal para más tarde comparar el comportamiento con esos modelos y poder detectar las anomalías.

Dependerá de la organización, pero para crear un modelo por ejemplo se debe recolectar y capturar datos de estos elementos:

- Dispositivos conectados; portátiles, tablets, móviles, servidores etc.
- La configuración de hardware de los dispositivos conectados.
- La configuración de los dispositivos de infraestructura de red; routers, switches, firewalls, etc.
- Tráfico de los segmentos de red, cuanto tráfico es normal, ancho de banda utilizado, horarios de tráfico etc.
- Componentes del sistema operativo, sesiones iniciadas, encendidos y apagados.
- Navegadores web, plugins instalados, componentes normalmente utilizados en la red.
- Aplicaciones utilizadas.

- Infraestructura de máquinas virtuales, incluidos los proveedores en la nube.
- Conexiones de colaboradores y de puntos de acceso remotos.
- Puntos de acceso de internet.
- Todas las DMZ y las VLAN.
- Servicios empresariales como DNS, LDAP y Active Directory.

Con toda la información de actividad de estos elementos capturada y almacenada, se puede crear un modelo de funcionamiento normal, con el que comparar el tráfico y encontrar anomalías.

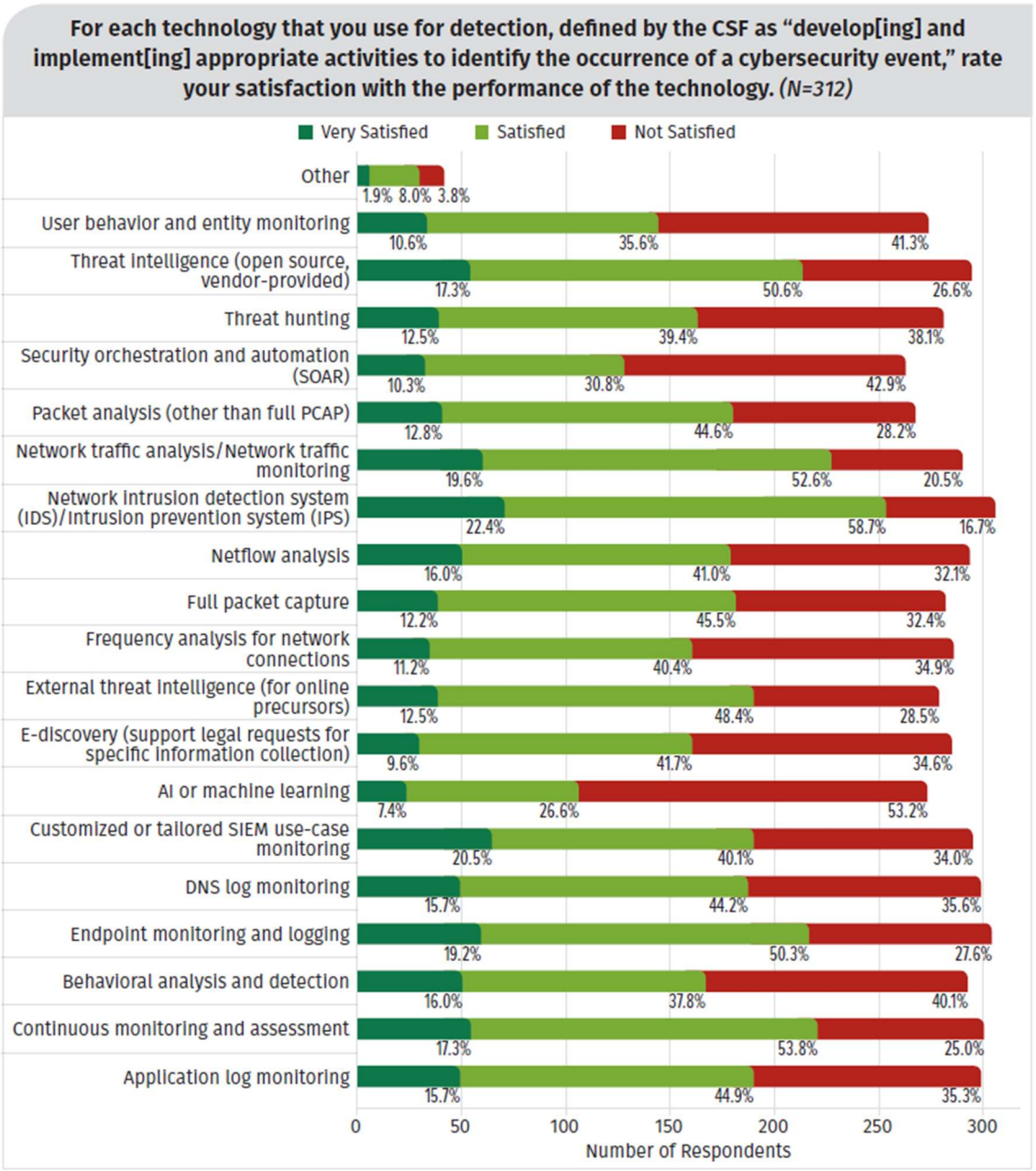


Ilustración 40: Ejemplo de tecnologías de detección utilizadas y su grado de satisfacción [24]

[24] Edición de 2019 del informe SANS Security Operations Center (SOC)

5.2 Detección de intrusiones

El proceso de Identificación de amenazas necesita la captura y procesamiento de mucha información, es por ello que es necesario automatizar el proceso, para esa función

5.2.1 Detección de intrusiones (IDS)

Un IDS (Intrusion Detection System) es una herramienta para la detección de acceso no autorizados a una red o sistema, generando una alerta o log para que sea revisador por un analista del SOC. El IDS únicamente alerta de un posible ataque, no realiza ninguna acción de contramedida. A diferencia de un IDS un IPS (Intrusion Prevention System), que también se utilizan para la protección de una organización en un SOC, al detectar la intrusión realiza una acción programada según el tipo de ataque, para prevenirlo o incluso llegar a mitigarlo.

Para la detección de amenazas los IDS se basan en el uso de reglas, analiza el tráfico de red y cuando una consecución de eventos cumple una de las reglas crea un aviso. Estas reglas pueden ser creadas por el personal del SOC como parte del conocimiento adquirido en otros ataques, o aportadas por la comunidad como parte del conocimiento colectivo.

Para realizar está función se utilizan dos enfoques.

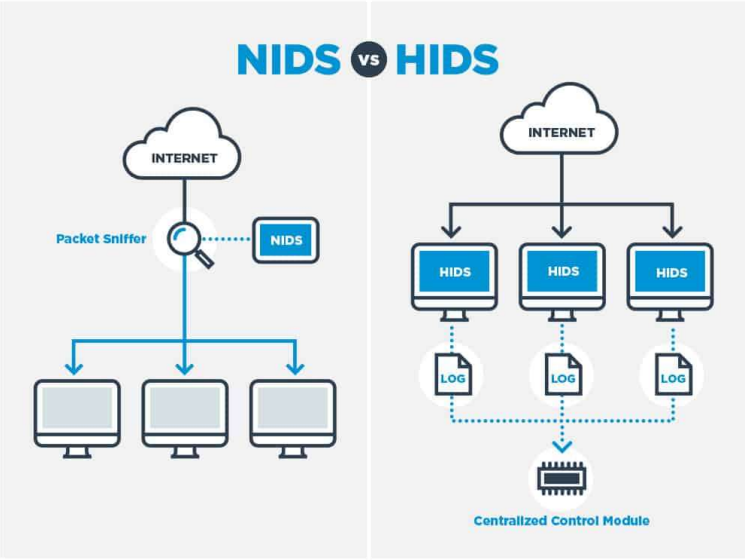


Ilustración 41: Esquema de funcionamiento de un NIDS y un HIDS[25]

[25]https://dementium2.com/administrador-neto/sistemas-de-deteccion-de-intrusiones-explicados-12/

5.2.2 Detección de intrusiones en red (NIDS)

Un NIDS (Network intrusión Detection System) es un sistema de detección de intrusos en red, analizando el tráfico en tiempo real intenta detectar anomalías que supongan un riesgo potencial. Normalmente este tipo de sistemas funcionan mediante reglas, que pueden ser personalizadas y ampliadas por el personal del SOC, existen repositorios de reglas generados por la comunidad que pueden ser utilizados, además de existir repositorios privados de reglas generadas por empresas para la detección de ataques concretos. Una vez que detecta una anomalía puede realizar acciones para mitigarla no únicamente se ocupa de informar.

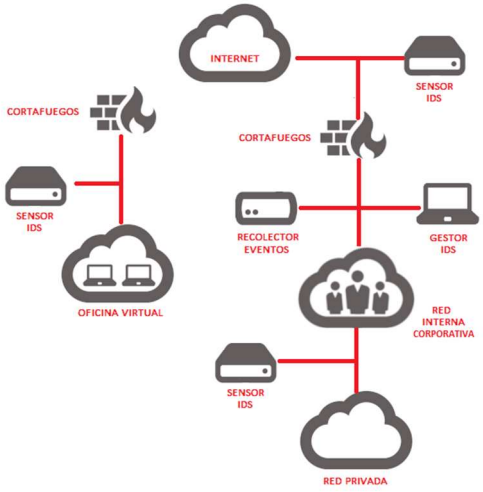


Ilustración 42: Esquema de Sensores Ids en una red[26]

Existen numerosos NIST de código abierto tales como Snort, Suricata o Zeek.

5.2.3 Detección de intrusiones basadas en host (HIDS)

Mediante un user agent se analiza el host, comprobando la configuración y el comportamiento del sistema, con este análisis se pueden identificar los equipos que han sido comprometidos, y cuando sea necesario, activar respuestas automáticas. Entre otras las capacidades principales de los agentes son:

- Recogida de datos de registros y eventos
- Monitorización de la integridad de archivos y claves de registro
- Inventario de procesos en ejecución y aplicaciones instaladas
- Supervisión de los puertos abiertos y de la configuración de la red
- Detección de rootkits o artefactos de malware
- Evaluación de la configuración y supervisión de políticas
- Ejecución de respuestas activas

Los agentes se pueden ejecutan en muchas plataformas diferentes, como Windows, Linux, o Mac OS X. Normalmente pueden ser configurados y gestionados desde el servidor del SOC.

[26] https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

Según el sistema operativo podemos encontrar diferentes HIDS, por ejemplo Wazuh tiene versiones para los principales sistemas operativos, o en el caso de Windows podemos utilizar la colección de herramientas Sysinternals[27] para monitorizar los equipos.

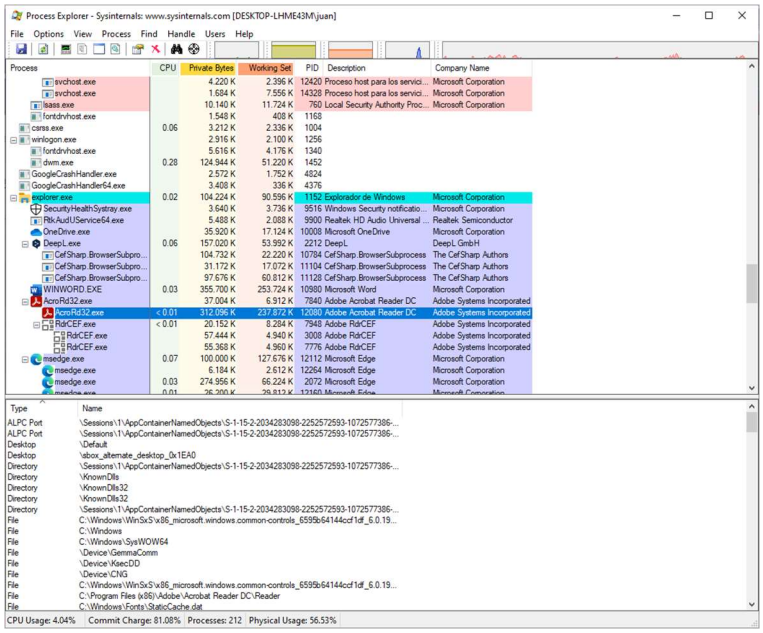


Ilustración 43: Herramienta Process Explorer de sysinternals

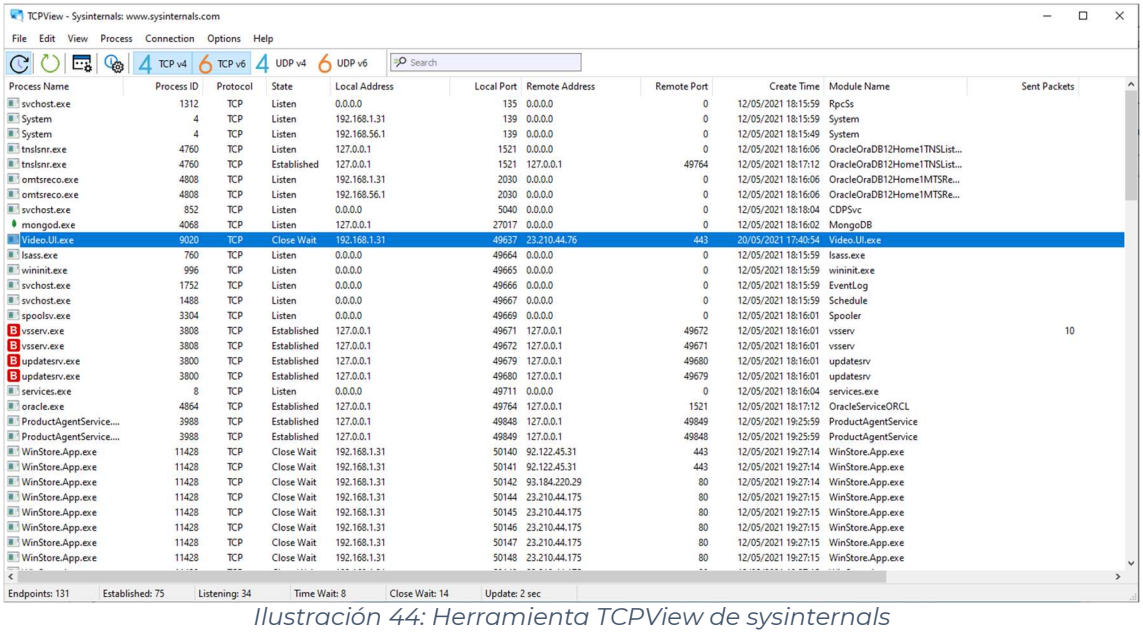


Ilustración 44: Herramienta TCPView de sysinternals

[27] https://docs.microsoft.com/es-es/sysinternals/

5.3 Identificación de las amenazas en nuestro SOC

Security Onion dispone de múltiples herramientas para la detección de amenazas, tanto a nivel de red como de hosts, en nuestro SOC utilizaremos las siguientes.

5.3.1 Detección de intrusiones en red en nuestro SOC.

Como ya se ha mencionado anteriormente, Security Onion es una distribución Linux que engloba diferentes herramientas ejecutándose en contenedores dockers, esto permite la interrelación de las herramientas. En este caso es Security Onion quien recolecta el tráfico de la red por una interface específico para ello, y envía los paquetes a las herramientas que los necesiten.

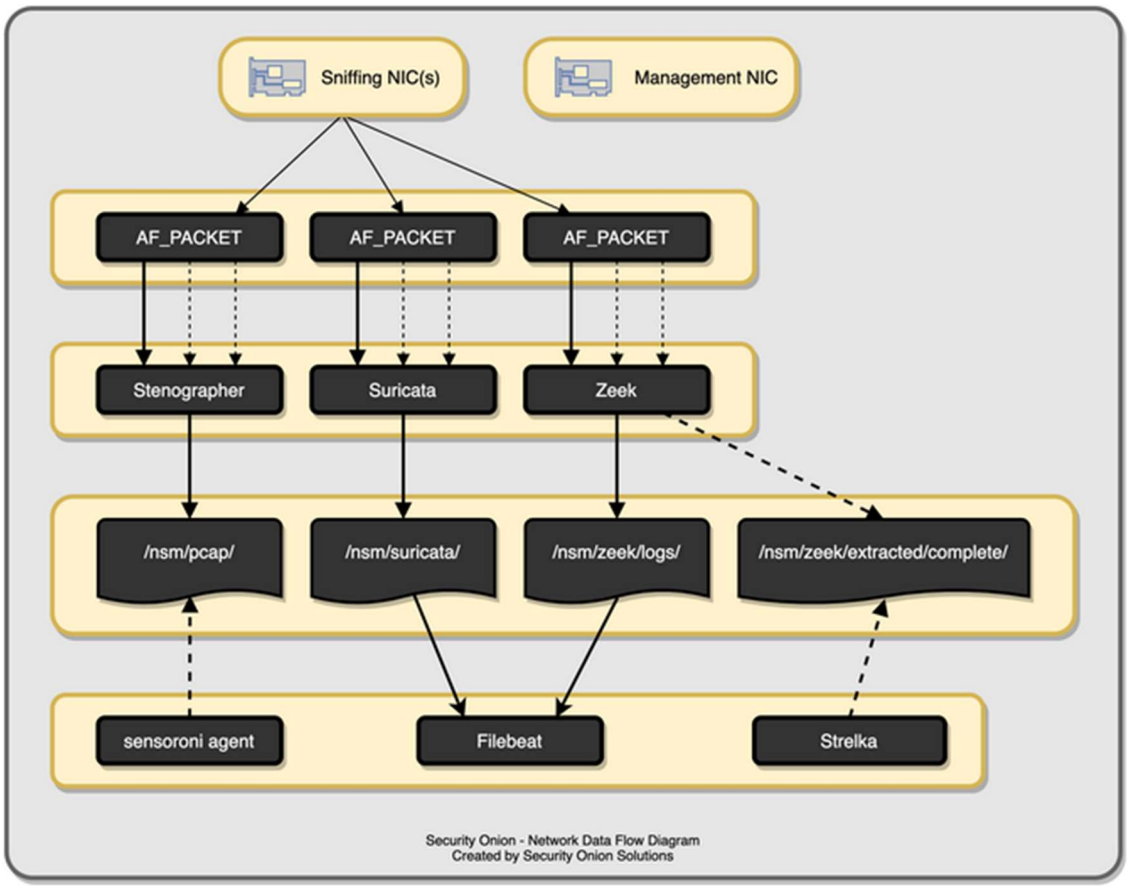


Ilustración 45: Diagrama de flujo de los datos de red

El flujo del tráfico es el siguiente:

- AF-PACKET: levanta tres servicios para la lectura del tráfico captura de la red, funciona como una especie de balanceador de carga, de forma que cada una de las instancias reciba el tráfico.
- El trafico llega a Stenographer[28] quien lo almacena para posteriores tareas de auditoría.
- El tráfico también llega a Suricata[29], que es un NIDS, quien lo procesa y en caso de alerta, la envía al dashboard del SIEM.

[28] https://github.com/google/stenographer
[29] https://suricata-ids.org/

- El tráfico también llega a Zeek[30], que es otro NIDS, que igual que Suricata lo procesa y en caso de alerta lo envía al dashboard.
- Zeek además envía los metadatos de los ficheros presentes en el tráfico a Stelka[31] que es un escáner en tiempo de ficheros, en busca de amenazas.

5.3.1.1 Suricata

Suricata es un NIDS con un motor de detección de amenazas de red maduro, rápido y robusto, de código abierto y gratuito. El motor de Suricata es capaz de detectar intrusiones (IDS) en tiempo real, prevenir intrusiones (IPS) en línea, monitorear la seguridad de la red (NSM) y procesar pcap fuera de línea.

Suricata inspecciona el tráfico de red utilizando un potente y extenso lenguaje de reglas y firmas, y cuenta con un potente soporte de scripts Lua para la detección de amenazas complejas. Security Onion descarga las reglas desde un repositorio de código abierto, pero los analistas del SOC pueden editarlas y crear reglas nuevas. O se pueden descargar desde repositorios privados.

Con formatos de entrada y salida estándar como YAML y JSON, se facilita la integración con herramientas como SIEMs existentes, en nuestro caso con Security Onion, las alertas emitidas por suricata se muestran en el dashboard.

El proyecto y el código de Suricata son propiedad y están respaldados por la Open Information Security Foundation (OISF), una fundación sin ánimo de lucro comprometida a garantizar el desarrollo y el éxito sostenido de Suricata como proyecto de código abierto.

5.3.1.2 Zeek

Zeek es el nuevo nombre del extensamente usado Bro[32] ,es un analizador de tráfico de red pasivo y de código abierto. Se puede utilizar como monitor de seguridad de la red (NSM) para apoyar las investigaciones de actividades sospechosas o maliciosas. Genera un amplio conjunto de registros que describen la actividad de la red. Estos registros incluyen no sólo un registro exhaustivo de cada conexión sino también transcripciones de la capa de aplicación. Éstas incluyen todas las sesiones HTTP con sus URIs solicitadas, cabeceras clave, tipos MIME y respuestas del servidor; solicitudes DNS con respuestas; certificados SSL; contenido clave de las sesiones SMTP; y mucho más.

Zeek almacena toda la información generada en archivos de registro bien estructurados y separados por pestañas o en formato JSON, adecuados para el post-procesamiento con software externo. En nuestro caso será Security Onion quien consume, almacena, procesa y presenten los datos para su consulta.

[30] https://zeek.org/
[31] https://github.com/target/strelka
[32] http://www.icir.org/robin/rwth/bro-intro.pdf

Además de los registros, Zeek incluye funciones integradas para una serie de tareas de análisis y detección, como la extracción de archivos de sesiones HTTP, la detección de malware mediante la interfaz con registros externos, la notificación de versiones vulnerables de software observadas en la red, la identificación de aplicaciones web populares, la detección de ataques de fuerza bruta a SSH, la validación de cadenas de certificados SSL y mucho más. Estos datos son enviados a Stelka para su procesamiento

No es un sistema clásico de detección de intrusos (IDS) basado en firmas; aunque también admite esa funcionalidad estándar, el lenguaje de scripting de Zeek facilita un espectro mucho más amplio de enfoques muy diferentes para encontrar actividad maliciosa. Entre ellos se encuentran la detección semántica de usos indebidos, la detección de anomalías y el análisis del comportamiento.

Zeek analiza el tráfico sin ser un analizador de protocolos como por ejemplo Wireshark, se complementa con Suricata para aumentar el rango de detección porque trabaja en otro nivel. Además, genera metadatos para que puedan ser analizados por Stelka.

5.3.1.3 Stelka

Strelka es un sistema de exploración de archivos en tiempo real, que se utiliza para la caza y detección de amenazas, y la respuesta a incidentes. Basado originalmente en el diseño establecido por Laika BOSS de Lockheed Martin y otros proyectos similares. Es una plataforma modular de exploración de datos, que en nuestro caso recibe archivos a través de Zeek provenientes del tráfico de la red, con el fin de analizar, extraer y elaborar informes sobre el contenido y los metadatos de los archivos. Junto con Security Onion, es capaz de agregar, alertar y proporcionar a los analistas la capacidad de comprender mejor su entorno sin tener que realizar una recopilación directa de datos o un análisis de archivos que requiera más tiempo.

5.3.2 Detección de intrusiones en host en nuestro SOC

Además de las herramientas de detección en red, Security Onion incorpora herramientas de detección en host, recopila la información de diferentes tipos de agentes, en el servidor y la procesa para que esté disponible para los analistas.

5.3.2.1 Wazuh

Wazuh es un proyecto de código abierto que proporciona visibilidad de seguridad, cumplimiento y capacidades de monitorización de la infraestructura. El proyecto nació como una bifurcación de OSSEC HIDS y ha evolucionado hasta convertirse en una solución completa implementando nuevas funcionalidades e integrando herramientas adicionales como Elasticsearch.

Wazuh se compone de dos partes, el servidor y el agente. El agente se instala en los hosts y recopila la información, que envía al servidor donde se almacenan y se muestran para que estén disponibles para el analista.

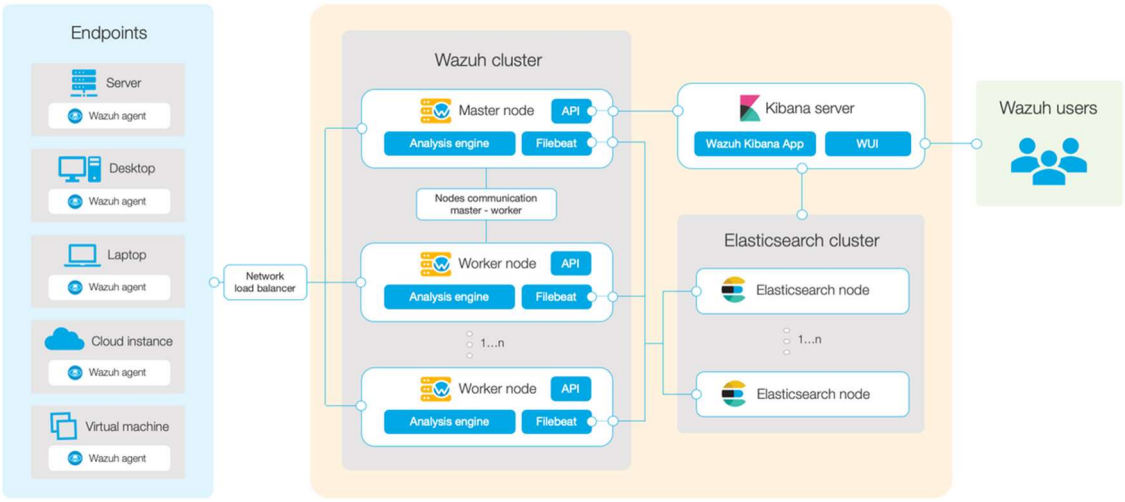


Ilustración 46: Esquema de funcionamiento de Wazuh

El servidor Wazuh se basa en un conjunto de aplicaciones donde cada aplicación o componente está diseñado para realizar una determinada tarea. Estos componentes trabajan juntos para:

- analizar los datos recibidos de varios registros,
- activar alertas cuando un evento de registro coincide con una regla
- registrar nuevos clientes/agentes
- enviar datos al servidor de Elastic Stack.

El gestor de Wazuh recibe y analiza los datos de los agentes utilizando decodificadores y reglas que han sido creadas para activar las alertas de seguridad. El gestor también se utiliza para distribuir archivos de configuración a los agentes, para supervisar su estado y para enviar mensajes de control para desencadenar acciones automáticas a nivel de agente.

El servicio de registro utiliza un mecanismo seguro para registrar agentes sin ninguna intervención del lado del servidor.

La API RESTful proporciona una interfaz para gestionar y supervisar la configuración del gestor y los agentes. Puede utilizarse para registrar agentes, inspeccionar los mensajes de registro del gestor, los descodificadores y las reglas, y proporcionar información útil relacionada con los agentes, incluido su estado, detalles del sistema operativo y alertas relacionadas con la supervisión de la integridad de los archivos y las comprobaciones de raíz.

Filebeat se utiliza para reenviar los datos de las alertas del gestor Wazuh a Elasticsearch. Este componente tiene su propia documentación desarrollada por Elastic.

El agente Wazuh se ejecuta en los hots y se encarga de recopilar datos de registro y eventos, realizar escaneos de monitorización de políticas, detectar malware y rootkits y activar alertas cuando se modifican los archivos

monitorizados. Se comunica con el servidor Wazuh a través de un canal cifrado y autenticado.

El agente esta compuesto de las siguientes partes:

- Rootcheck realiza la detección de rootkits y malware en todos los sistemas en los que está instalado el agente.
- Log monitoring/analysis recoge y analiza los registros del sistema en busca de cualquier actividad sospechosa.
- Syscheck se ejecuta periódicamente para comprobar si hay cambios en cualquier archivo configurado (o entrada del registro en Windows).

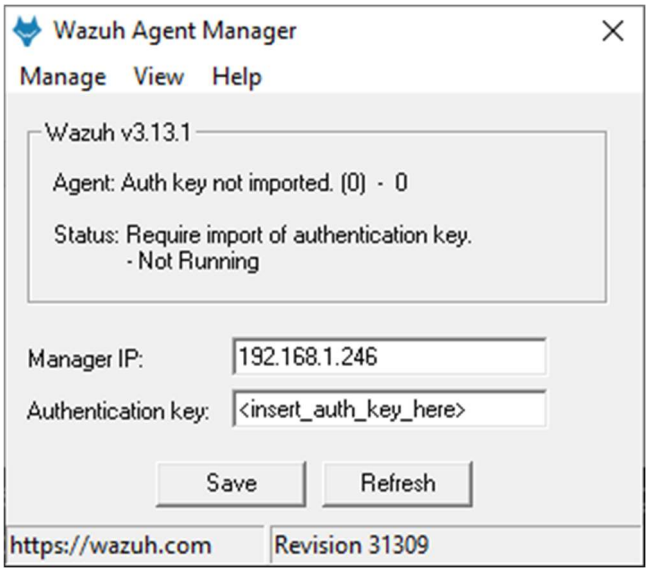


Ilustración 47: Ventana del agente de wazuh en windows

5.3.2.2 Autoruns y Sysmon

Para los sistemas Windows, que son la mayoría de los hosts de la organización, existen agentes que aportan información del estado del sistema, ya implementados en el propio sistema operativo, Security Onion integra la comunicación con estos agentes para recabar esta información.

5.3.2.2.1 Autoruns

Esta utilidad, que tiene el conocimiento más completo de las ubicaciones de inicio automático de cualquier monitor de inicio, muestra qué programas están configurados para ejecutarse durante el arranque o el inicio de sesión del sistema, y cuando se inician varias aplicaciones integradas de Windows como Internet Explorer, el Explorador y los reproductores multimedia. Estos programas y controladores incluyen los de la carpeta de inicio, Run, RunOnce y otras claves del Registro. Autoruns informa sobre las extensiones del shell del Explorer, las barras de herramientas, los objetos de ayuda del navegador, las notificaciones de Winlogon, los servicios de inicio automático y mucho más. Autoruns va mucho más allá de otras utilidades de autoinicio.

Toda esta información es enviada al servidor del SOC para procesarla y poder identificar posibles amenazas en el arranque de Windows.

5.3.2.2.2 Sysmon

System Monitor (Sysmon) es un servicio del sistema Windows y un controlador de dispositivo que, una vez instalado en un sistema, permanece residente a través de los reinicios del sistema para supervisar y registrar la actividad del sistema en el registro de eventos de Windows. Proporciona información detallada sobre la creación de procesos, conexiones de red y cambios en el tiempo de creación de archivos. Recogiendo los eventos que genera mediante la Recogida de Eventos de Windows o los agentes SIEM y analizándolos posteriormente, puede identificar la actividad maliciosa o anómala y comprender cómo operan los intrusos y el malware en su red.

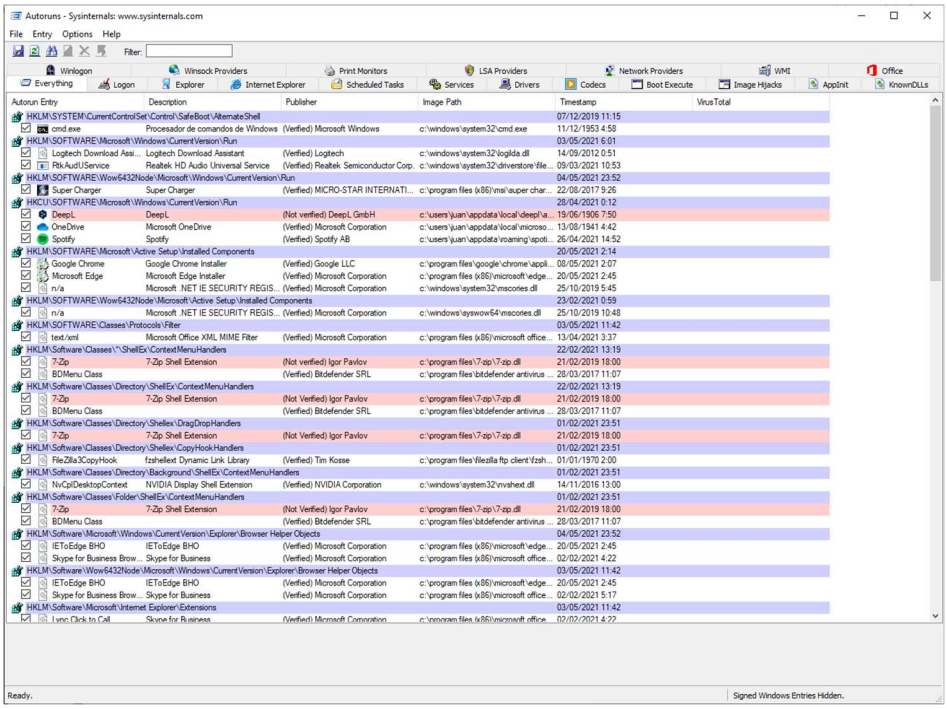


Ilustración 48: Agente de Autoruns

5.3.3 ATT&CK Navigator

Para ayudar al analista a identificar posibles amenazas, el dashboard de Security Onion incorpora una web con la matriz de ATT&CK, el analista puede consultarla para buscar posibles correlaciones entre ataques conocidos y eventos detectados en el SOC.

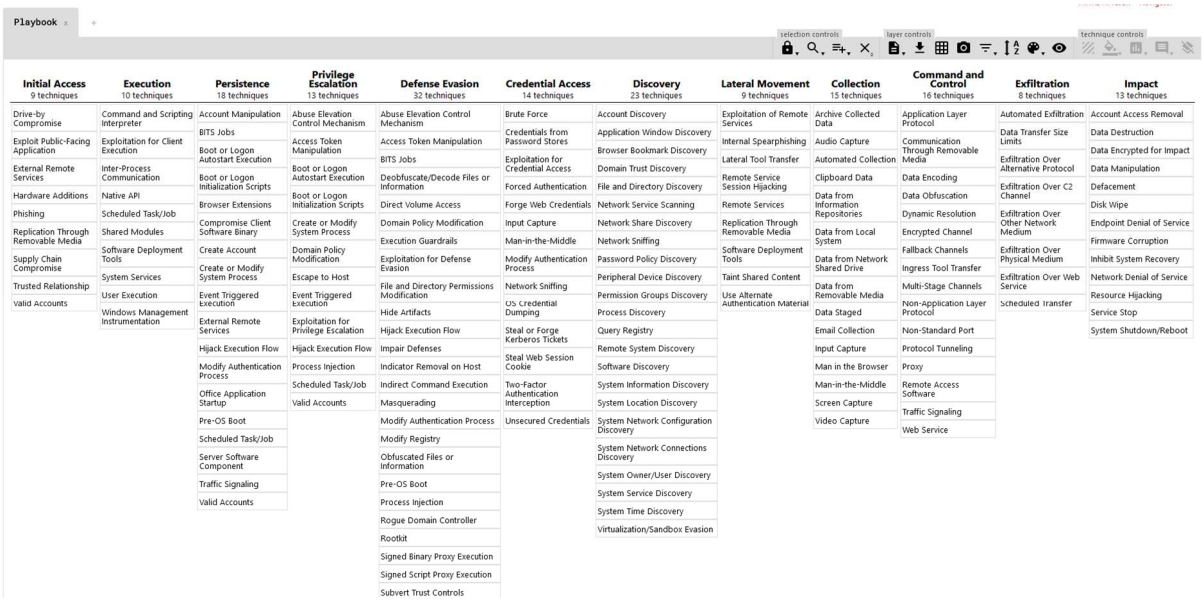


Ilustración 49: Matriz ATT&CK

5.3.4 Dashboard de Security Onion

Toda la información de los NIDS y los HIDS es enviada a la consola de Security Onión, quien tiene dos apartados específicos para mostrar las anomalías detectadas, Alerts y Hunts.

5.3.4.1 Alerts

La interfaz de alertas da una visión general de las alertas que Security Onion está generando y permite profundizar rápidamente en los detalles, pivotar a Hunt o PCAP, y escalar las alertas a TheHive[33].

Esta interface permite una visión rápida de los eventos que han sido detectados, para facilitar al analista el triaje y detectar cuales son una posible amenaza real, en ese caso se puede cambiar a otra interface que aporte mayor información.

[33] https://thehive-project.org/

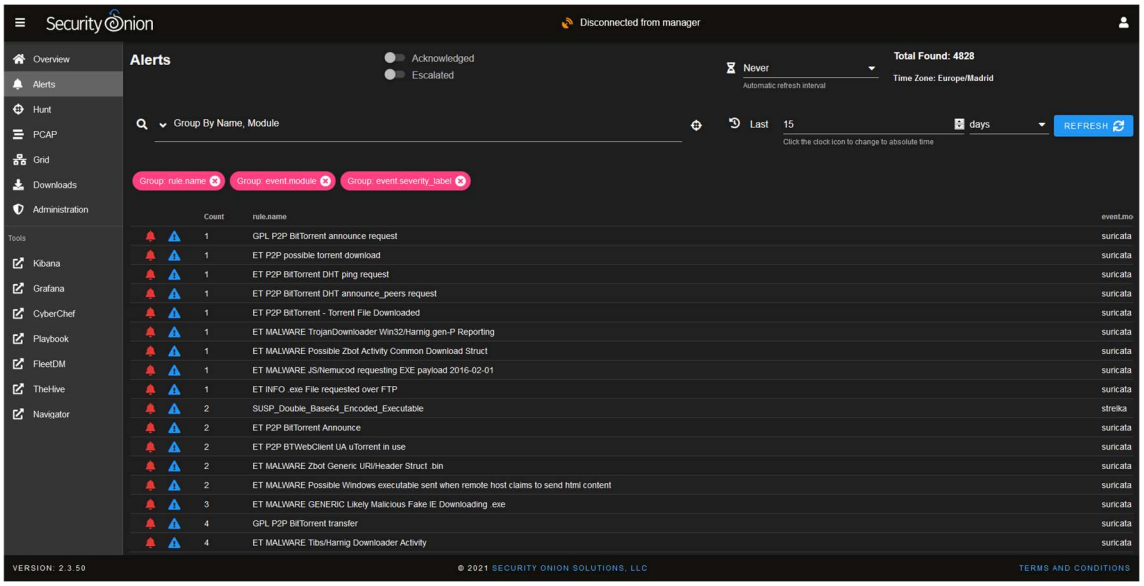


Ilustración 50: SOC ventana de alertas

5.3.4.2 Hunt

La interface Hunt le permite cazar todos los datos de Elasticsearch y está muy ajustada para apilar, pivotar, ampliar y reducir los datos.

En esta interface se obtiene más información de los eventos, se pueden relacionar datos, y realizar búsquedas más precisas.

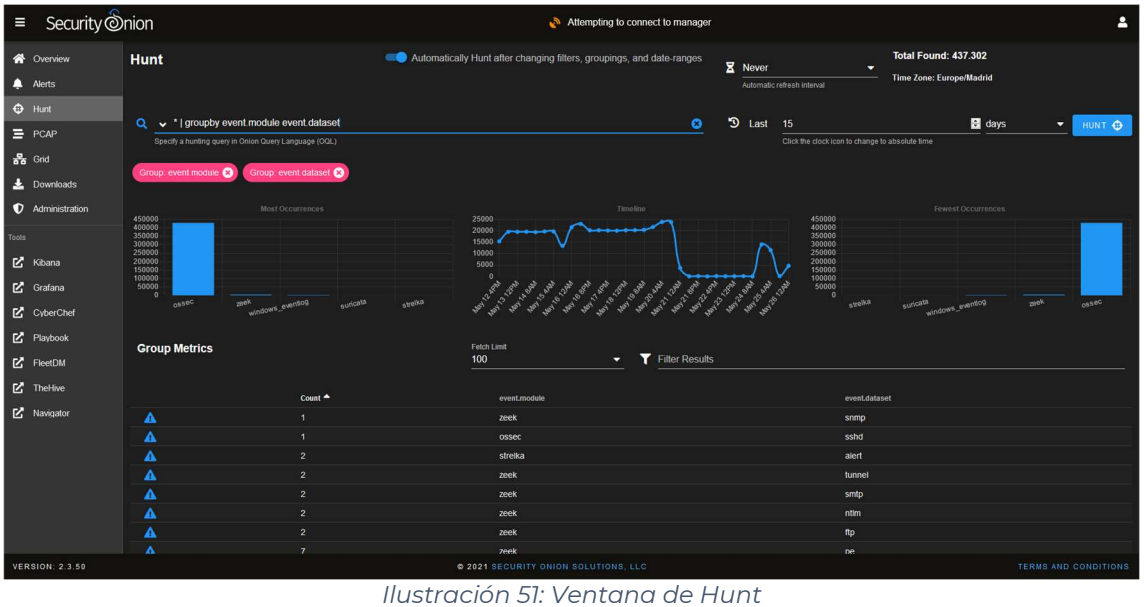


Ilustración 51: Ventana de Hunt

6. Brechas de seguridad

Una vez que ya sabemos que activos pueden ser vulnerables en nuestra organización, también sabemos que es lo normal y podemos detectar anomalías, tenemos que saber a detectar las brechas de seguridad. Una anomalía puede o no significar un ataque, y un ataque no tiene por qué provocar una brecha de seguridad, si hemos hecho bien el trabajo nuestro sistema debe de ser capaz de repeler el ataque sin provocar daños a la organización, pero esto no siempre se puede asegurar.

6.1 Hay que prepararse para lo peor

No existe un sistema totalmente seguro, no se pueden evitar todas las brechas de seguridad. Por más esfuerzos y recursos que destinemos a bastionar un sistema nunca se pueden cerrar todas las posibles vías de ataque, nosotros somos los que somos, y es el mundo el que nos ataca, seguro que, a alguien, en algún lugar, se le ocurre un nuevo vector de ataque en el que no habíamos caído, o encuentra una vulnerabilidad que no se conoce y decide explotarla.

Hay que tener claro que siempre existe la posibilidad de sufrir un incidente de seguridad y deberemos de estar preparados para ello. La gestión de riesgos es una parte de la política de seguridad que la empresa tiene que tener, como por ejemplo gestionar el enfrentarnos a tener que tomar la decisión de cuál es la rentabilidad de parar un proceso crítico para la continuidad de negocio al encontrar una vulnerabilidad en algún activo que lo soporte. El tener un seguro contratado que nos cubra de las posibles pérdidas, o cuales son los pasos a dar en el caso que un ataque por ransomware encripte los archivos de la empresa y produzca una filtración de información. Los ciberdelincuentes son conscientes de esto, que muchas veces la operatividad de la organización está por delante de la seguridad, y no se adoptan todas las medidas necesarias para que no se vea afectada, y siempre intentan obtener beneficio de ello. Para intentar que la hipotética ventaja que adquieren gracias a esta cuestión sea la menor posible, es importante detectar las brechas de seguridad tan pronto como sea posible.

Ilustración 52: Pantalla del ransomware wannacry

6.2 Detección de brechas de seguridad análisis forense.

Cuando los sistemas de detección de intrusos avisan de que existen comportamientos anómalos, es necesario que conozcamos el comportamiento de nuestros sistemas para poder identificar las brechas de seguridad reales, lo que ya hemos comentado de disponer de una variable, con la que poder comparar y utilizarla para detectar cambios y poder investigarlos. Las herramientas vistas en el tema anterior nos proveen de esa variable y nos avisan cuando se detectan anomalías, es aquí cuando entra el analista de nivel dos. Se han de estudiar las anomalías y saber interpretarlas, utilizar herramientas forenses para analizar los datos e identificar las brechas. Analizar los cambios en los hosts, estudiar los paquetes de tráfico sospechoso, las conexiones anómalas, o que no deberían de existir. Un SOC tiene que estar preparado para realizar este trabajo, bien de manera local, o bien de forma externa.

Todo el trabajo realizado hasta ahora se basa en comprender el comportamiento de la organización y todos los sistemas que la componen, comprender como se comunican los elementos entre sí, que servicios se ejecutan y que protocolos se usan. Para posteriormente con este conocimiento poder detectar cualquier brecha de seguridad. Deberemos de en nuestra implementación del SOC ser capaces de contestar a las siguientes preguntas:

- ¿Como detectar si un activo está comprometido, si no he sido capaz de detectar el ataque?
- ¿Si he sufrido un ataque como debo tratar el incidente para paliar los efectos?

6.3 Monitorización de comportamiento

Para poder contestar a estas preguntas se ha de monitorizar constantemente los sistemas de la organización. La información que se obtiene de la monitorización de los sistemas, utilizando las herramientas de análisis, se ha de interpretar con cuidado. Es muy complicado poder afirmar que los sistemas de la organización se puedan predecir, picos temporales de trabajo, pruebas de herramientas nuevas o nuevos equipos en la red pueden generar comportamientos no vistos antes haciendo soltar las alarmas. Por estos motivos se han de tener información de diferentes herramientas y una herramienta donde se centralice y se pueda analizar.

Se pueden aplicar diferentes enfoques para la monitorización de nuestra organización. Pero en realidad son prácticamente los mismos que para la detección de intrusos, realmente el enfoque es la utilización de estas herramientas en el análisis y detección de las brechas.

6.3.1 Monitorización activa del servicio

Mediante un latido periódico comprueba que los servicios en el host continúan ejecutándose. Mediante está sincronización a nivel de red valida el funcionamiento y además obtiene una respuesta en el caso que por algún motivo dejen de estar disponibles. Por ejemplo, esa es una de las funciones del agente de Wazuh

6.3.2 Análisis de datos de red

Captura el tráfico de red para poder analizar los metadatos, pero a nivel de protocolos, como, por ejemplo, sesiones HTTP con sus URIs solicitadas, cabeceras clave, tipos MIME y respuestas del servidor. También permite calcular el ancho de banda utilizado y detectar anomalías en él. Por ejemplo, estas son las funciones de Zeek.

6.3.3 Captura de tráfico

Esnifar y almacenar los paquetes TCP/IP que circulan por la red. Esto da la posibilidad de posteriormente realizar un análisis forense del tráfico e inspeccionarlo en profundidad en búsqueda de indicios de brecha de seguridad.

6.3.4 Detección de intrusiones basadas en host

Un agente instalado en el host monitoriza los procesos, los recursos utilizados del host y además puede detectar anomalías, como procesos nuevos o actividades anómalas, que pueden ser indicativos de un ataque. Por ejemplo, está sería el cometido tanto de Wazuh, como de la recolección de los datos de Autorun y Sysmon.

Como se puede ver, la detección de brechas es el siguiente paso de la detección de anomalías y como ya hemos comentado, consiste en analizar esas anomalías para determinar si en realidad se ha producido un incidente de seguridad, utilizando herramientas forenses, y actuar frente al incidente.

6.4 Análisis forense

El análisis forense utilizar procesos científicos previamente establecido para recopilar, analizar y presentar evidencias. Es un método que combina partes de derecho y de informática para recopilar y analizar datos de sistemas informáticos, y presentarlos de forma que sean admisible como prueba en un proceso judicial. Asegurando la cadena de custodia y todas las garantías legales.

En un SOC el análisis forense tiene la función de identificar como ha ocurrido la brecha de seguridad y aportar tanto las pruebas por si hubiera que iniciar un proceso judicial, como la información del modus operandi para evitar que vuelva a ocurrir, con lo cual en un SOC se deben tener analistas formados en análisis forense, y en caso que fuera necesario darle entidad de evidencias judiciales llamar a un perito forense colegiado para esas tareas.

Para realizar un análisis forense son necesarias herramientas de análisis. Las herramientas de análisis forense son relativamente nuevas. Con la evolución de los dispositivos, el aumento de conexiones y equipos conectados entre sí, el análisis manual se convirtió en una tarea mucho más compleja e improductiva. También los ataques se volvieron más sofisticados de forma que podían reducir su huella, interviniendo el dispositivo sin modificarlo, esto hizo necesario la creación de herramientas automáticas y potentes.

Muchas herramientas son polivalentes e implementas varias funciones a la vez. Esto es una tendencia importante en las herramientas forenses digitales, que sean una especie de navaja suiza para los analistas y peritos forenses, que les permitan multitud de recursos en una misma herramienta, para facilitar su labor de campo, ya que pueden estas investigando un dispositivo y tener que ejecutar otra herramienta o cambiar de una a otra puede suponer un problema, al solo disponer de una herramienta se facilita mantener la cadena de custodia.

Dentro de las herramientas forenses la más conocida es Autopsy[34], que es una plataforma forense digital y una interfaz gráfica para la herramienta Sleuth Kit, que es de la misma empresa, y de otras herramientas forenses digitales. Es muy utilizada por investigadores y fuerzas del orden, para investigar lo que ocurrió en un dispositivo, o recuperar información de una unidad de memoria.

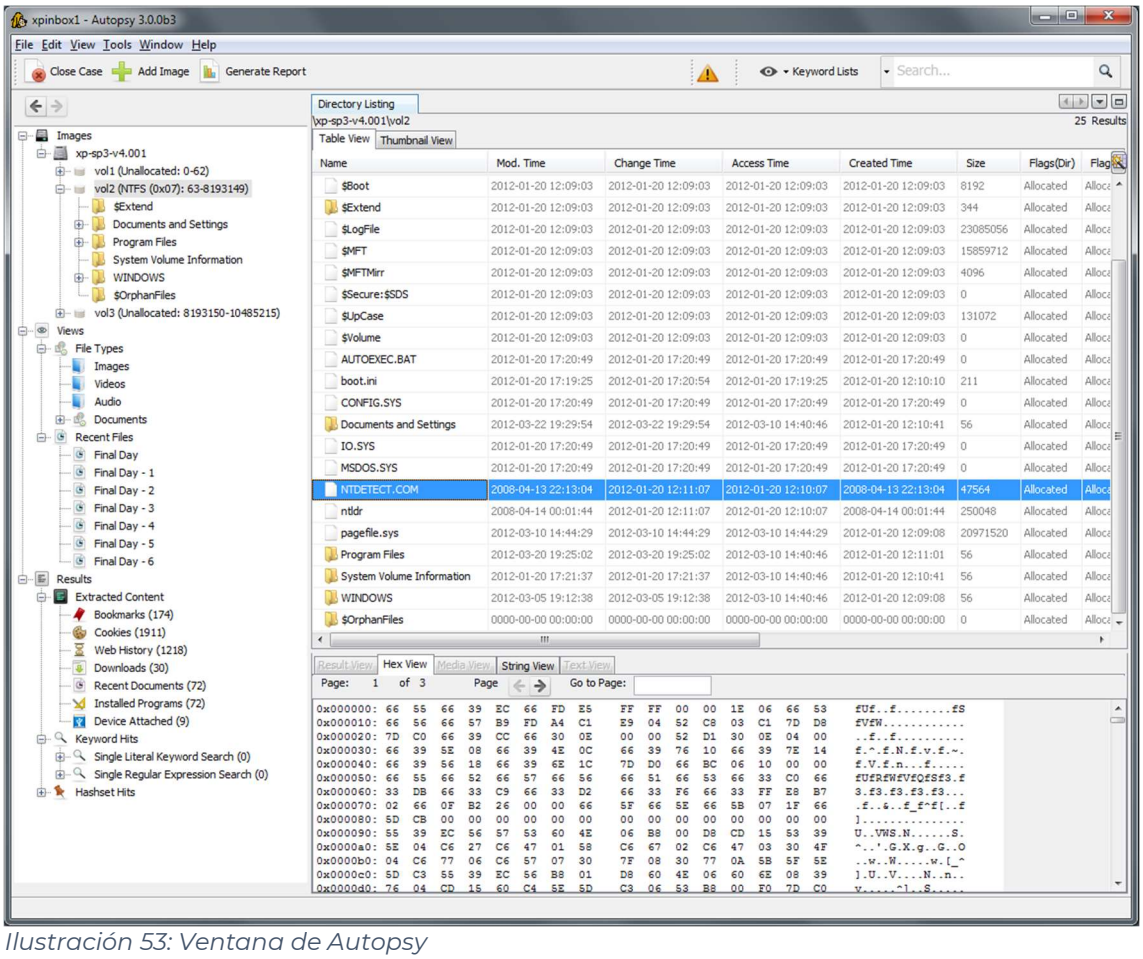


Ilustración 53: Ventana de Autopsy

[34] http://www.sleuthkit.org/autopsy/

Incluso se han creado distribuciones Linux específicas para análisis forense, donde ya vienen instalas y configuradas las principales herramientas, como por ejemplo Sift[35] (SANS Investigative Forensic Toolkit) desarrollada por una agrupación internacional de expertos forenses, con apoyo del SANS. Este tipo de distribuciones dotan a los analistas y peritos forenses, de un entorno especializado con una colección de herramientas para realizar todas las labores que sean necesarias. Sift tienen herramientas para realizar operaciones como el montado de imágenes, creación de líneas de tiempo, recopilación de memoria volátil o efímera y el uso de herramientas como Sleuthkit o Autopsy.

Ilustración 54: Captura de pantalla de la distribución Sift de SANS

6.5 Respuesta a un incidente de seguridad.

Una vez se produce una brecha de seguridad, hay que dar respuesta al incidente de seguridad producido. Cada organización junto con el SOC, deben establecer un plan de respuesta a los incidentes, según el tipo de organización y los tipos de incidente a los que se puede ver expuesta. Es el SOC quien determina las amenazas a las que se enfrenta la organización, al definir los activos que hay que proteger y cuales son vulnerables.

Ilustración 55: Fases de la respuesta a incidentes.

[35] https://www.sans.org/tools/sift-workstation/

En las fases 3 y 4 del manejo de incidentes de seguridad, como ya se ha tratado en este trabajo de fin de master, se ha de dar respuesta al incidente, no existe un mecanismo estándar para la resolución de incidentes, según la organización y el tipo de incidente el procedimiento cambiará, existen guías de buenas prácticas para la resolución como la del NIST[36]. El SOC debe tener personal especializado en la resolución de incidentes, además de conocimientos de análisis forense y junto con la organización planes para actuar en caso de que exista una brecha de seguridad, esta última parte debe de esta incluida en el SGSI de la organización.

6.6 Detección de brechas de seguridad en nuestro SOC.

En nuestro SOC, Security Onion integra las herramientas de detección de incidencias que se muestran en el SIEM, que ya vimos en el apartado anterior, que nos permiten detectar posibles anomalías por parte del analista de nivel 1, para que sean estudiadas por el analista de nivel 2 y si es necesario realizar un análisis forense. Para realizar un análisis forense incorpora varias herramientas que utilizaremos.

6.6.1 Wireshark y NetworkMiner

En el apartado *3.4.1 Descubrimiento mediante escaneo pasivo de la red*, se explica que Security Onion almacena el tráfico y se puede descargar en formato pcap, para analizar estos datos, incorpora dos aplicaciones, NetworkMiner, que ya fue comentada en el mismo apartado y Wireshark.

Wireshark es quizás el analizador de protocolos de red más importante. Es muy utilizado para análisis de datos y protocolos, para solucionar problemas en redes o como una herramienta didáctica. Es una herramienta similar a tcpdump[37], pero dispone de interfaz gráfica y más opciones, de filtrado y organización de la información.

Incluye las siguientes funciones:

- Inspección en profundidad de cientos de protocolos, a los que se añaden otros constantemente
- Captura en vivo y análisis fuera de línea
- Navegador de paquetes estándar de tres paneles
- Multiplataforma: Funciona en Windows, Linux, macOS, Solaris, FreeBSD, NetBSD y muchos otros.
- Los datos de red capturados pueden explorarse a través de una interfaz gráfica de usuario o mediante la utilidad TShark en modo TTY
- Los filtros de visualización más potentes del sector
- Análisis de VoIP enriquecido
- Lee/escribe muchos formatos de archivos de captura diferentes
- Los archivos de captura comprimidos con gzip pueden descomprimirse sobre la marcha
- Se pueden leer datos en vivo de diferentes tipos de protocolos.

[36] https://doi.org/10.6028/NIST.SP.800-184
[37] https://www.tcpdump.org/

- Soporte de descifrado para muchos protocolos, incluyendo IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP y WPA/WPA2
- Se pueden aplicar reglas de coloreado a la lista de paquetes para un análisis rápido e intuitivo
- Los resultados se pueden exportar a XML, PostScript®, CSV o texto sin formato

En nuestro SOC lo utilizaremos para analizar paquetes sospechosos y para funciones de análisis forense.

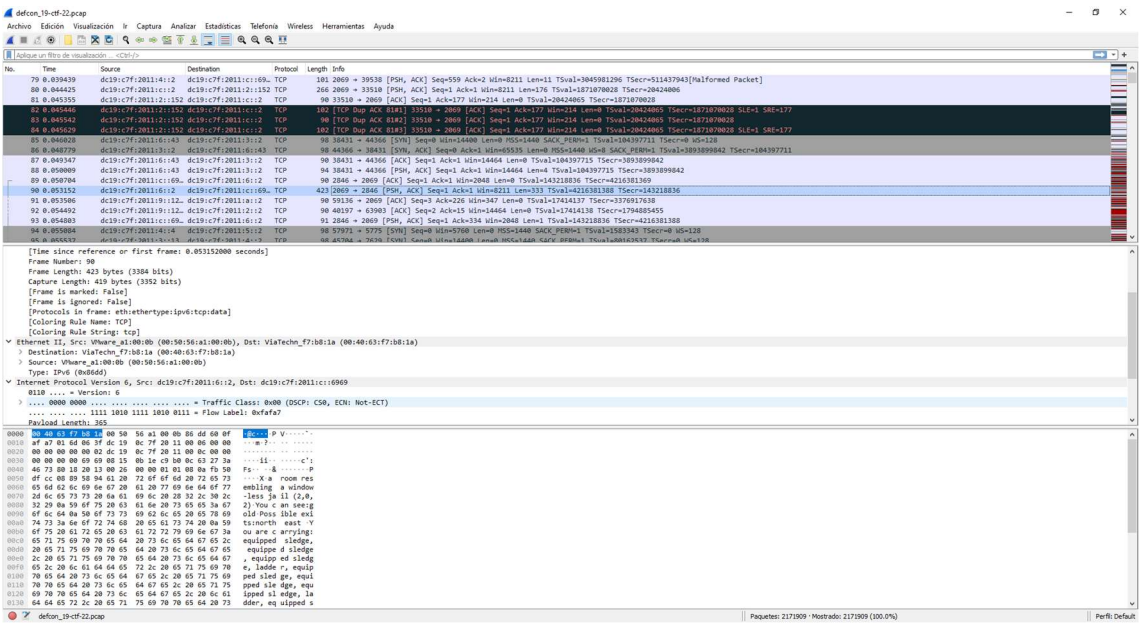


Ilustración 56: Pantalla de wireshark

6.6.2 CyberChef

CyberChef[38] es una herramienta web para realizar operaciones informáticas, nos permitirá analizar, convertir y decodificar diferentes tipos de dato, sin necesidad de utilizar múltiples herramientas ni tener que programar en lenguajes de programación para realizar diferentes acciones.

Permite realizas más de 100 operaciones entre datos, como, por ejemplo, codificar una cadena en formato Base64, y también decodificar una cadena Base64 a texto plano. Es capaz de realizar cálculos de direcciones IPv4 y IPv6. También puede realizar funciones hash de los datos introducidos, soporta los algoritmos MD5, SHA1, SHA224, SHA256, SHA512 y SHA3. También soporta cifrado de algoritmos AES, Blowfish, DES, 3DES e incluso implementa PBKDF2 como XOR o Base64, además de muchas otras conversiones.

En nuestro SOC la utilizaremos como herramienta para ayudarnos a procesar la información que encontremos en los paquetes de datos, realizar conversiones e intentar obtener la información en plano de posibles datos ofuscados.

[38] http://icyberchef.com/

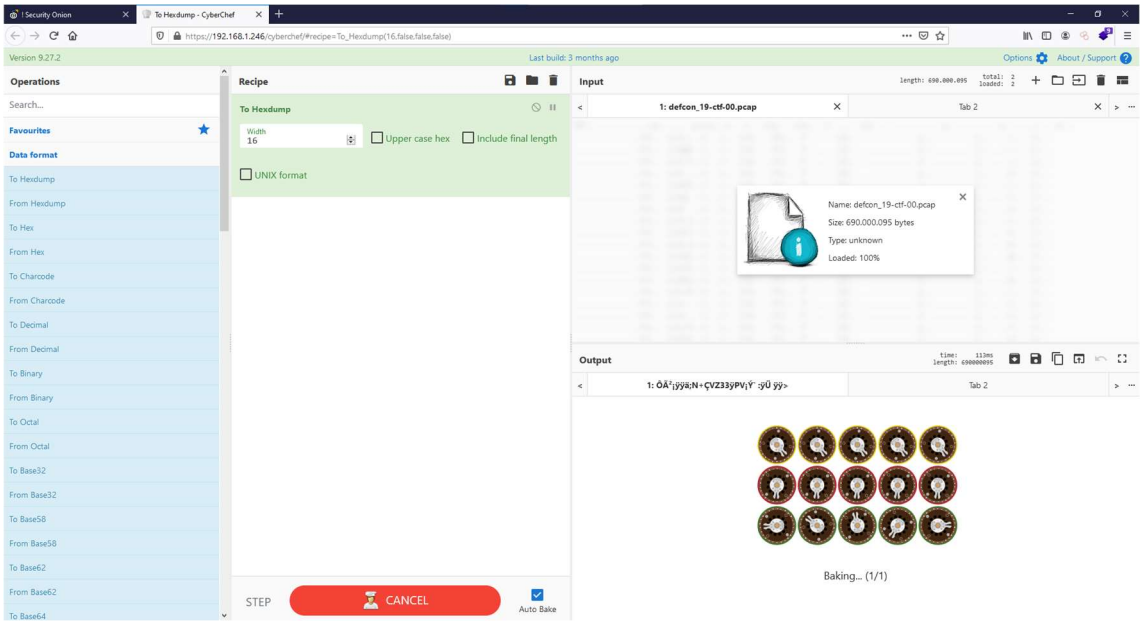


Ilustración 57: Pantalla de CyberChef

7 Análisis de los datos

Al implementar las herramientas tratadas en este trabajo de fin de master, descubrimiento de activos, análisis de vulnerabilidades, detección de anomalías y la monitorización del comportamiento, generan una gran cantidad de datos, que deben ser estudiados por los analistas. Estos necesitan mecanismos de automatización para poder analizarlos en un plazo de tiempo razonable. Además, los datos deben evaluarse en su contexto con el resto de los datos generados, para poder darles un significado. También es necesario la normalización los datos que provienen de diversas fuentes, para que puedan ser relacionadas entre sí es las mismas condiciones.

7.1 El contexto es lo más importante.

El contexto se puede definir como las circunstancias que forman la configuración, para un evento, declaración o idea y en términos de lo cual puede ser plenamente comprendido y evaluado. La información del contexto es junto con la capacidad de almacenamiento y la memoria RAM de los equipos, son las cosas que los equipos del SOC nunca consideran tener suficiente. En las operaciones de seguridad a largo plazo, es de falta de contexto la carencia a la que más se tiende. Es complicado obtener y almacenar todo el contexto que rodea a cada uno de los eventos.

Para la seguridad de la mayoría de organizaciones, no existe ningún recurso que por si miso, actualmente proporcione suficiente información de contexto, o funcionalidad para tomar una decisión informada. Durante años se han ido añadiendo recursos a una mezcla de herramientas, que han dado como resultado un lio de eventos, alarmas, alertas, paquetes capturados, detección de sistemas de protección, recursos IDS, gestores de seguridad empresarial, análisis de big data, herramientas personalizadas etc.

El trabajo en un SOC para tomar decisiones informadas, requiere de grandes cantidades de datos, en un espacio temporal definido, en un formato normalizado y contexto adecuado, que requieren una reflexión crítica día tras día. En su trabajo el SOC debe hacer frente a la falta de información y al esfuerzo fragmentado entre múltiples recursos, para poder componer una imagen amplia de la situación de la organización.

Muchas veces es posible que el SOC tenga que hacer conjeturas basadas en datos imperfectos, y tengas que advertir que los análisis realizados se han hecho sin suficiente información para hacer un análisis preciso.

7.2 Toma de decisiones.

Para la toma de decisiones, es necesario disponer de la mayor cantidad de información posible, disponer del contexto de esta la información, para actuar de forma más eficiente con los recursos de los que se dispone y crear un plan de actuación que maximice la seguridad de la organización. Por ejemplo, si se detecta una brecha de seguridad en un host de la red, deberemos saber qué servicios se ejecutan en ese host y que servicios dependen de él, que hosts se pueden ver afectados por la brecha o hasta dónde puede llegar la infección. Se deberá tener toda la información posible para tomar las mejores decisiones, si es más conveniente atajar la brecha, o proteger primero los hosts que se puedan ver afectados, y dejar al atacante actuar para observar su modus operandi, para identificar el vector de ataque y poder tomar medidas futuras. O es mejor solucionar la brecha de seguridad y que el atacante no siga afectando al sistema.

La capacidad de encontrar el sentido a estos datos, poder organizarlos y ponerlos en contexto, requiere un sistema que los consolide y los gestione todos. Una herramienta que ayude a contestar las siguientes preguntas:

- ¿Cuáles son las acciones que van a tener más impacto en la seguridad de mi organización?
- ¿Qué es lo primero que debo hacer?
- ¿Cuáles son los datos prioritarios para monitorizar?

7.3 El SIEM

Para la comprensión y correlación de los datos se ha desarrollado la tecnología SIEM (Security Information & Event Management), que es la unión de dos tecnologías SEM (gestión de eventos de seguridad) y SIM (gestión de información de seguridad).

El SIEM es una plataforma diseñada para gestionar la información, evaluar los eventos y la información de seguridad. Dispone de la facultad de normalizar y analizas los datos provenientes de diferentes herramientas y correlacionarlos para presentarlos ante el analista y facilitarle la detección de eventos de seguridad.

La principal característica de un SIEM es la eficacia con la que es capaz de correlacionar y presentar los datos recopilados. El propósito esencial de esta plataforma es facilitar y permitir una mayor eficacia del trabajo de los analistas en el análisis de la gran cantidad datos con los que trabaja. Pero para que el analista pueda entender el significado de los datos, es necesario ponerlos en contexto con el resto de los datos procesados y con los datos que se tienen almacenados; no obstante, es necesario para aumentar la eficacia en el trabajo diario del analista que la plataforma sea capaz de automatizar la correlación. de los datos, para conseguir detectar conductas maliciosas, actividades anómalas e indicios que no indiquen que existe una brecha de seguridad. Es importante que nuestra plataforma SIEM disponga de mecanismos de actualización, de los últimos conocimientos de amenazas, para que esta

correlación permita detectar los métodos más innovadores de los ciberdelincuentes y las metodologías del software malicioso.

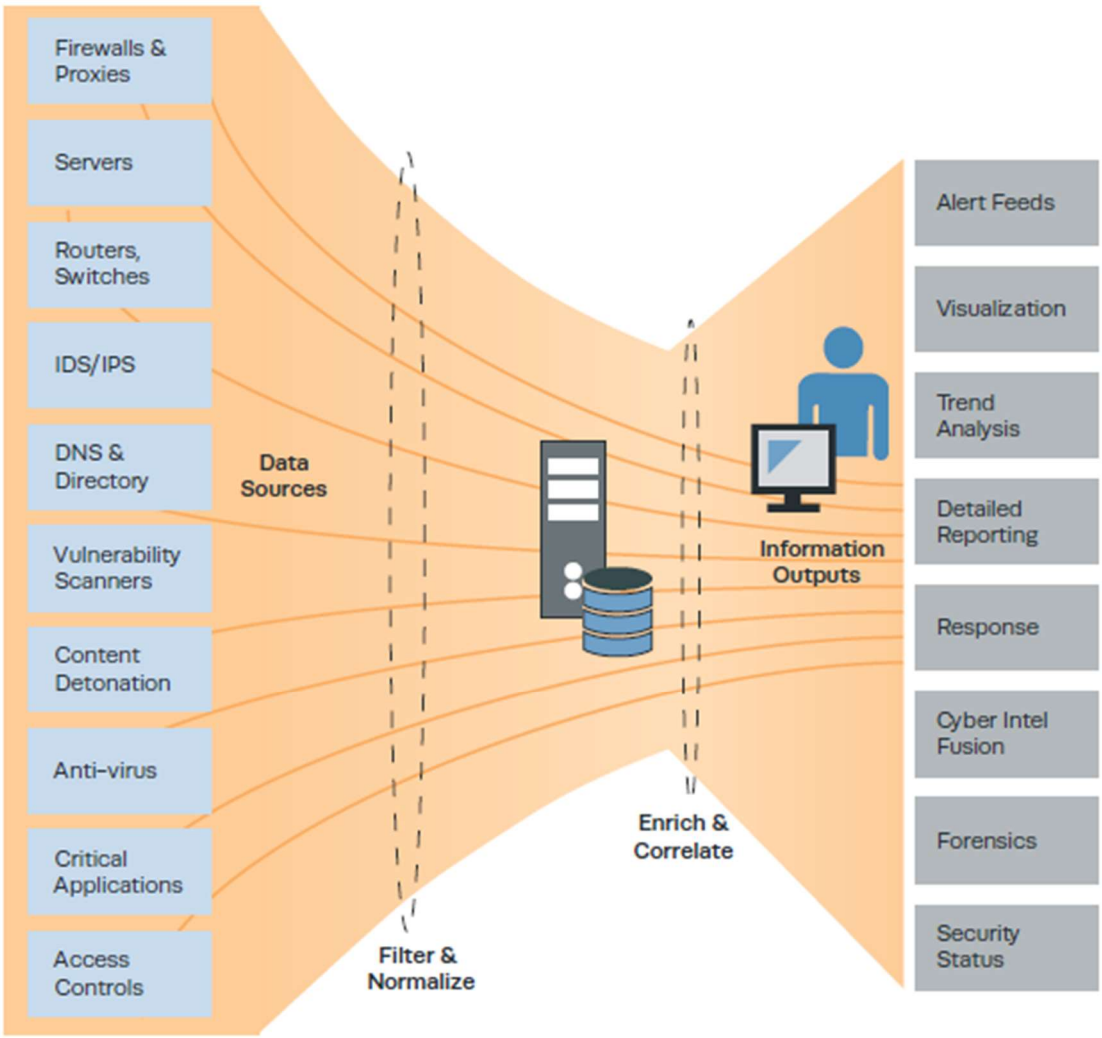


Ilustración 58: Estructura de un SIEM

7.3.1 Funcionamiento de un SIEM

Un SIEM es el controlador lógico de un SOC, no existe una estructura estándar para un SIEM, al final es un conjunto de partes (IDS, Host Agents, firewall) que general información y que son orquestadas por el SIEM. Quien de forma simplificada se puede definir como un sistema gestor de logs, al cual según la organización se le van agregando herramientas y funciones para aumentar sus capacidades en la gestión de la seguridad de dicha organización.

De forma simple se podría describir el flujo de trabajo de un SIEM con la siguiente secuencia:

- Un agente recoge información de uno o varios dispositivos, estos datos con normalizados y se les asigna un nivel de criticidad por el agente, y los envía a SIEM.
- Los datos son almacenados en un servidor central, aunque muchos SIEM pueden estar distribuidos, como simplificación se puede suponer que se almacenan en una base de datos centralizada.

- El SIEM filtra la información recibida según diferentes criterios, información redundante, filtros creados por los analistas etc.
- El SIEM pasa los datos ya normalizados por un motor de correlación en tiempo real aplicando reglas de defensa de la red, amenazas internas, cumplimiento de la normativa y otros casos de uso con el fin de detectar comportamientos anómalos o detectar posibles incidentes.
- Tradicionalmente, el SIEM sólo aporta datos basados en eventos, como NetFlow, alertas de IDS y datos de registro. Los SIEMS pueden integrar herramientas externas permitiendo reunir datos de escaneo de vulnerabilidad, muestras de malware, telemetría de host o PCAP.
- Algunos SIEM disponen de funciones más avanzadas y pueden automatizar acciones complejas como resultado de reglas de correlación, como cambiar reglas en un firewall o desactivar una interface.
- Y para terminar los datos recibidos son almacenados para aumentar la base de datos de correlación, y para posibles labores de análisis forense en caso de detectar un incidente de seguridad. Y vuelve a comenzar el proceso.
- Los analistas acceden a los datos generados por el motor de correlación normalmente a través de una interface web, pero no por ello es el único método. Los SIEM permiten a los analistas herramientas de seguimiento de los incidentes, para controlar la fase que está hasta su resolución.

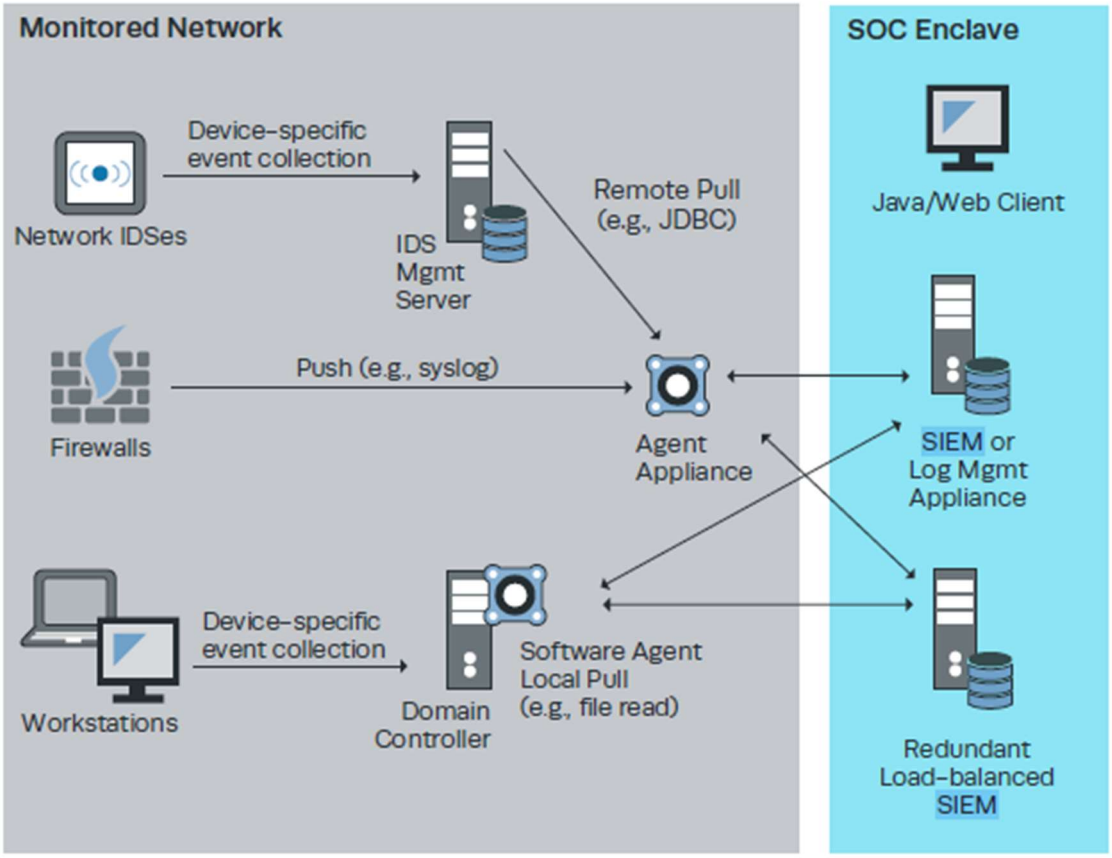


Ilustración 59: Estructura de datos de un SIEM

7.4 El SIEM en nuestro SOC

LA distribución de auditoría de redes que hemos instalado en el servidor de nuestro SOC, incorpora múltiples herramientas que ya hemos ido explicando a lo largo del trabajo. Como interfaz del SIEM incorpora lo que ellos denominan SOC (Security Onion Console), que es una interface web para la monitorización de los eventos y alarmas, además de las herramientas que incorpora para el analista. Divido en dos menús en el lateral izquierdo de la web.

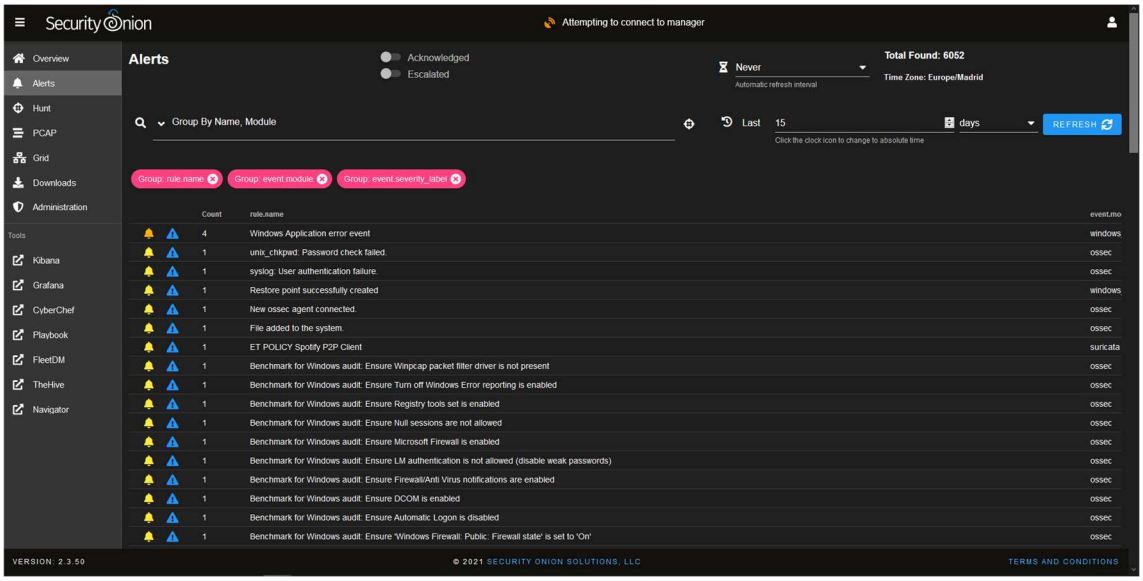


Ilustración 60: Pantalla de SOC de Security Onion

Security Onion como motor del SIEM utiliza Elasticsearch, que no es un motor del SIEM en sí, si no un motor de base de datos, al que se le pueden agregar módulos para la recolección de datos, visualización y correlación cubriendo con software de código abierto las principales funciones de un SIEM. En conjunto con el resto de herramientas que incluye Security Onion disponemos de un SIEM potente y totalmente funcional para un SOC implementado en una organización mediana o pequeña.

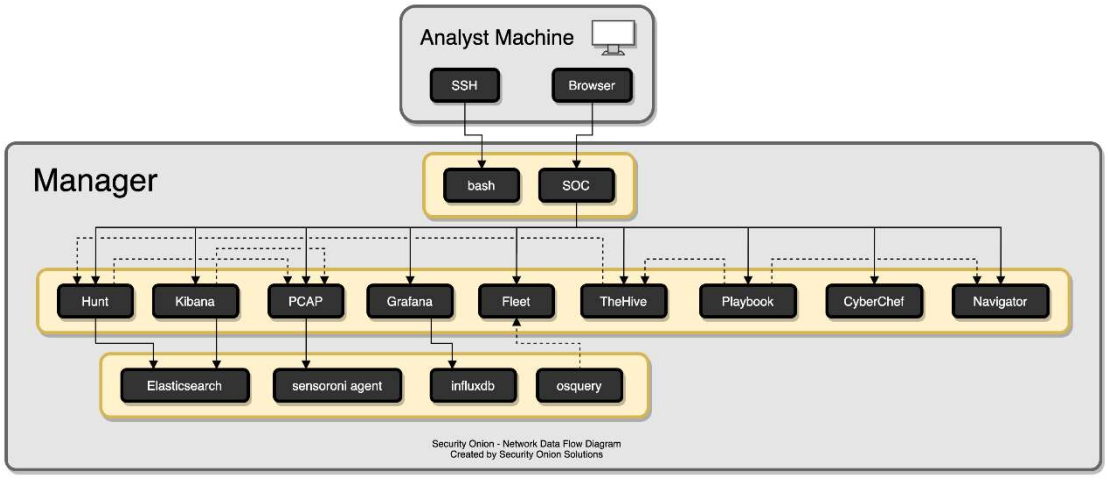


Ilustración 61: Diagrama del flujo de datos del SIEM de Security Onion

7.4.1 Funciones de Alerta.

En el menú de la izquierda nos podemos encontrar con las funciones de monitorización para el analista y de configuración del servidor de Security Onion. La descripción de las funciones es la siguiente:

- **Overview**: Muestra información sobre la versión actual de Security Onion y avisa de futuras actualizaciones.
- **Alerts**: ya se ha comentado en este trabajo, es la interface donde se pueden ver las alertas generadas en el SOC, permite una navegación rápida y cambiar a los menús de Hunt o PCAP o escalar una alerta a TheHive.
- **Hunt**: Permite una ampliación de los datos de las alertas vistas en el menú Alerts, permite navegar por todos los datos almacenados en Elasticsearch, ampliar, reducir y comparar para hacer correlaciones y búsqueda de contexto.
- **PCAP**: Este menú también lo hemos tratado ya, permite realizar búsquedas en todos los paquetes almacenados por Stenographer[39], y descargarlas en formato pcap para analizarlas con NetworkMiner y Wireshark.
- **Grid**: En nuestro caso Security Onion está instalado en un único servidor, pero permite la instalación distribuida en diferentes nodos, enviando toda la información a un servidor central. En este menú se tiene acceso a la red de los nodos instalados, obteniendo información de su estado.
- **Download**: En esta ventana podemos descargar los instaladores de diferentes agentes en la versión soportada por Security Onion, y para diferentes sistemas operativos.
- **Administración**: Panel de administración de los usuarios de la consola de Security Onion.

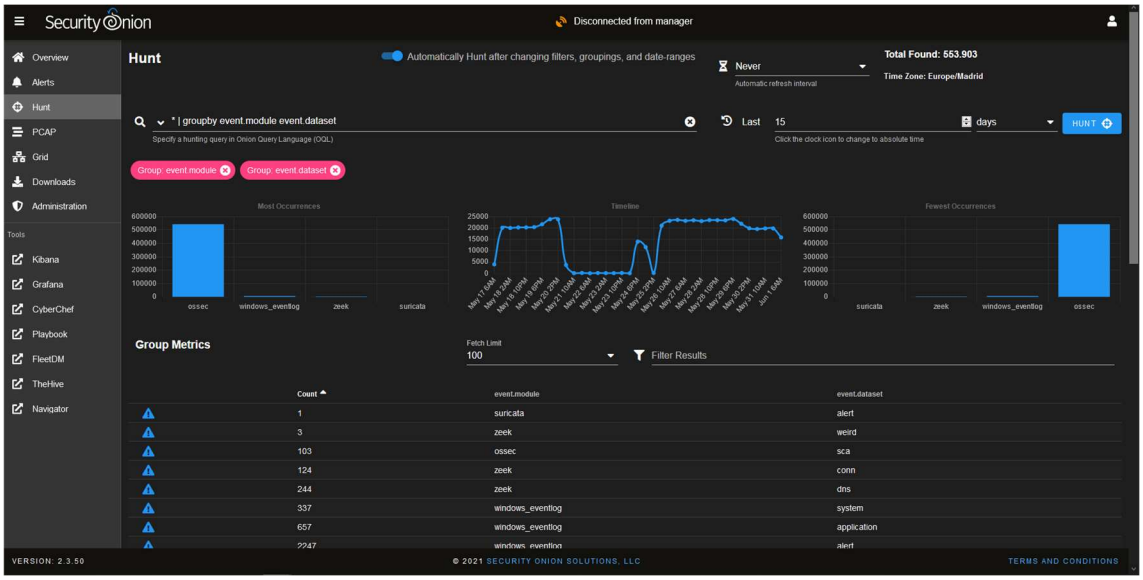


Ilustración 62: Ventana de Hunt de la consola de Security Onion

[39] https://docs.securityonion.net/en/2.3/stenographer.html#stenographer

7.4.2 Herramientas.

En la consola de security Onion también se tiene acceso directo a algunas de las herramientas que incorpora, algunas ya las hemos visto en apartados anteriores, pero otras no.

7.4.2.1 Kibana

Es una interfaz de usuario que permite la visualización de los datos de Elasticsearch y nagegar por Elastic Stack, da una interfaz de búsqueda y visualización de todos los datos almacenados por el SIEM, para poder realizar análisis, correlacionar datos y búsquedas de contexto. Es una herramienta muy potente, mucho más que Hunt.

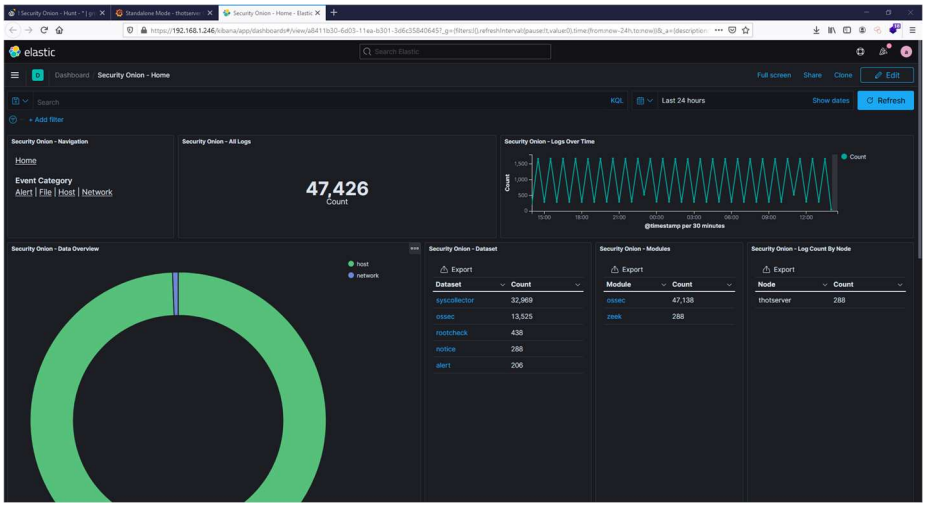


Ilustración 63: Dashboard de Kibana

7.4.2.2 Grafana

Es una interfaz también de Elasticsearch, pero permite la visualización de los datos del estado del servidor en formato gráfico para su mejor comprensión.

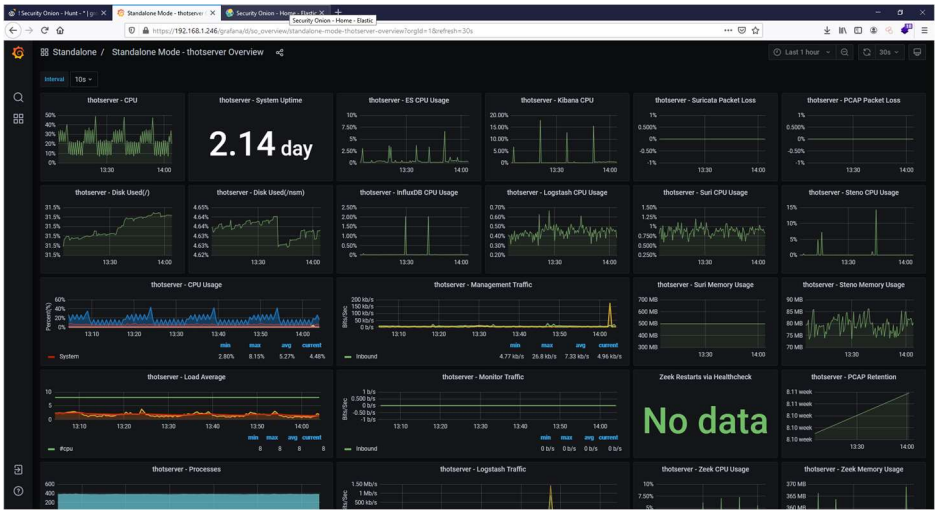


Ilustración 64: Interfaz de Grafana

7.4.2.3 Ciberchef

Esta herramienta ya ha sido explicada en este trabajo, es una herramienta web que permite la conversión de múltiples tipos de datos para facilitar al analista el estudio forense de la información.

7.4.2.4 Playbook

Es una aplicación web que se puede instalar en los nodos distribuidos. Permite crear un Playbook de detección en cada nodo, que a su vez consta de Plays individuales. Estos Plays son totalmente autónomos y describen los diferentes aspectos en torno a una estrategia de detección particular. Se pueden crear mediante scripts alertas de detección concretas, una especie de reglas, que crearán alertas que se enviarán al servidor central o en el caso de un único servidor aparecerán en los menús de alertas del SIEM.

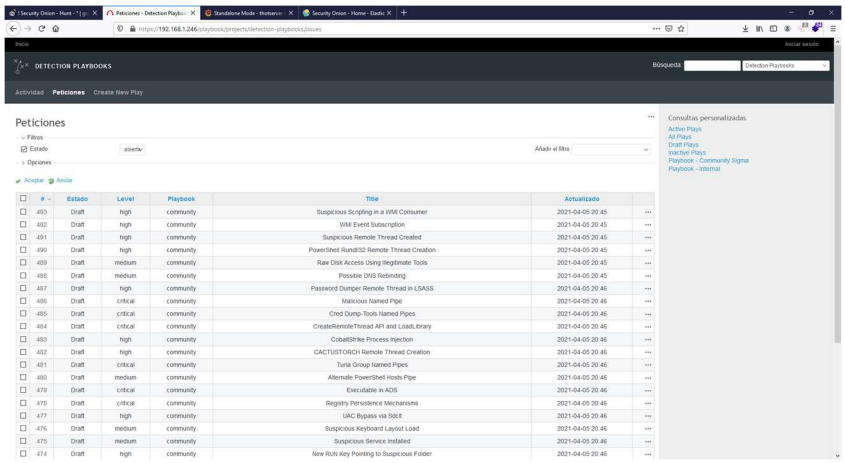


Ilustración 65: Interface de Playbook

7.4.2. 5 Fleet

Como ya se ha explicado en el apartado 3.4.2, es la interface web de Osquery, que permite realizar búsquedas en los hosts, sobre todos los elementos y servicios que los componen.

7.4.2.6 TheHive

Es una Plataforma de Respuesta a Incidentes de Seguridad escalable, de código abierto. Permite mantener el seguimiento de los incidentes por cualquier miembro del SOC. Además, mediante el uso del motor Cortex puede realizar un análisis del incidente utilizando más de 100 analizadores, pudiendo responder activamente a las amenazas y recibir información del colectivo Cortex. Está muy integrado en MISP, que es el estándar de facto para la comparación de amenazas, por ello puede exportar e importar casos para su investigación.

7.4.2.7 ATT&CK Navigator

Es una representación web de la matriz de Mitre ATT&CK, como ya se vio en el apartado 5.3.3

8. Formación del personal del SOC

Una de las partes más importantes a la hora de implementar un SOC, es el equipo, y su formación, debido al particular trabajo de analista de SOC, la formación y las capacidades del equipo deben de ser multidisciplinares, no todos los miembros deben tener los mismos conocimientos, y según se sube en el nivel de analistas, los conocimientos deben de ser más profundos y más específicos.

La formación del equipo dependerá de los servicios que ofrezca el SOC, deberá de disponer de personal cualificado para ellos, es por eso que es complicado mantener un SOC para una organización pequeña, debe de contratar a personal cualificado, con el costo que eso supone, es más económico subcontratar ciertos servicios a un SOC externo. De forma que siguiendo con la línea de todo lo que rodea al SOC, no existe un estándar de formación del personal, porque no todos los SOCs dan los mismos servicios, no tienen el mismo personal formado.

Además, la formación del personal es un proceso continuo, no solamente a nivel de estudios reglados y certificaciones, si no actualizados en nuevos vectores de ataques y formas de intrusión, deben estar informados de las nuevas vulnerabilidades descubiertas, y ser proactivos en la implementación de medidas de seguridad preventivas.

8.1 Nivel de formación del personal.

Intentando realizar una aproximación, a la formación que debería tener el personal podría ser esta:

8.1.1 Personal de la organización.

El punto más débil de cualquier organización suelen ser lo usuarios de la misma, da igual las medidas de seguridad que se implementen, si los propios integrantes de la organización no tienen una formación en seguridad informática, serán el principal vector de ataque. Desde el SOC deben dar formación para evitar que esto pase, e intentar reducir el vector de ataque que existe entre la pantalla del pc y la silla.

8.1.2 Tier 1

Es Operador del SOC, debe tener conocimientos sobre:

- Administración de sistemas.
- Redes de computadoras.
- Conocimientos de ciber seguridad.

Por ejemplo, podría estar en posesión de las certificaciones CompTIA Network+ y CompTIA Security+[40]

[40] https://certification.comptia.org/es/certificaciones?level=core

8.1.3 Tier 2

Es el responsable de determinar si el comportamiento anómalo es un ataque o no y dar la primera respuesta al incidente, debería de tener conocimientos sobre:

- Administrador de sistemas.
- Nivel avanzado de redes de computadoras.
- Análisis forense.
- Conocimientos de ciberseguridad.
- Conocimientos de análisis de malware.

Por ejemplo, podría tener la certificación CompTIA CySA+[41] o la Eccouncil Certified SOC Analyst (CSA)[42]

8.1.4 Tier 3

Es él analista de mayor rango, es un analista especializado en algún campo, como por ejemplo el forense, o experto de alto nivel en equipos de un fabricante en concreto, por ejemplo, debería disponer como formación las certificaciones del fabricante.

8.1.5 Supervisor del SOC

Es un cargo que necesita formación técnica de alto nivel, pero también formación administrativa, política y de gestión de equipos, debería de ser una persona con por ejemplo la certificación ISACA CISM (Certified Information Security Manager)[43]

8.2 Ejemplo de formación la Certificación CSA

Cada vez existen más formación específica para los analistas del SOC, sigue siendo un tema complejo, pero dentro de la arbitrariedad que rige a los SOCs, las múltiples guías de buenas prácticas, creadas por las entidades responsables de ciberseguridad de cada país o región, y los intentos de normalización, están creando unos perfiles comunes que deberían de haber en todos los SOCs, a pesar que según los servicios particulares de cada uno requieran una mayor especialización en algún área en concreto.

Dentro de esta formación, ponemos por ejemplo la certificación Certified SOC Analyst (CSA) de Eccouncil, que estaría orientada más o menos a un analista de nivel 2.

Según Eccouncil los objetivos de aprendizaje del CSA son los siguientes:

- Adquirir conocimientos sobre los procesos, procedimientos, tecnologías y flujos de trabajo del SOC.
- Adquirir una comprensión básica y un conocimiento profundo de las amenazas a la seguridad, los ataques, las vulnerabilidades, los

[41] https://www.comptia.org/certifications/cybersecurity-analyst
[42] https://www.eccouncil.org/programs/certified-soc-analyst-csa/
[43] https://engage.isaca.org/madridchapter/certificaciones/cism

comportamientos de los atacantes, la cadena de muerte cibernética, etc.
- Capaz de reconocer las herramientas, tácticas y procedimientos de los atacantes para identificar los indicadores de compromiso (IOC) que pueden ser utilizados durante las investigaciones activas y futuras.
- Capaz de supervisar y analizar registros y alertas de una variedad de tecnologías diferentes a través de múltiples plataformas (IDS/IPS, protección de puntos finales, servidores y estaciones de trabajo).
- Conocer el proceso de gestión centralizada de registros (CLM).
- Ser capaz de realizar la recopilación, supervisión y análisis de eventos de seguridad y registros.
- Adquirir experiencia y amplios conocimientos sobre la gestión de eventos e información de seguridad.
- Adquirir conocimientos sobre la administración de soluciones SIEM (Splunk/AlienVault/OSSIM/ELK).
- Comprender la arquitectura, implementación y puesta a punto de las soluciones SIEM (Splunk/AlienVault/OSSIM/ELK).
- Adquirir experiencia práctica en el proceso de desarrollo de casos de uso de SIEM.
- Ser capaz de desarrollar casos de amenaza (reglas de correlación), crear informes, etc.
- Aprender los casos de uso que se utilizan ampliamente en el despliegue de SIEM.
- Planificar, organizar y realizar la supervisión y el análisis de amenazas en la empresa.
- Ser capaz de monitorizar patrones de amenazas emergentes y realizar análisis de amenazas de seguridad.
- Adquirir experiencia práctica en el proceso de clasificación de alertas.
- Ser capaz de escalar los incidentes a los equipos apropiados para obtener asistencia adicional.
- Utilizar el sistema de gestión de tickets del servicio de atención al cliente.
- Preparar informes sobre la metodología de análisis y sus resultados.
- Conocer la integración de la inteligencia de amenazas en el SIEM para mejorar la detección y la respuesta a los incidentes.
- Capaz de hacer uso de información sobre amenazas variada, dispar y en constante cambio.
- Adquirir conocimientos sobre el proceso de respuesta a incidentes.
- Obtener una comprensión de la colaboración entre el SOC y el IRT para mejorar la respuesta a los incidentes.

Como se puede ver es un programa muy completo de formación específica de analista de SOC, pero antes de realizar este programa se ha de tener una formación de base, está pensado para que lo realicen:

- Analistas del SOC (Tier I and Tier II)
- Administradores de redes y seguridad, ingenieros de redes y seguridad, analistas de defensa de redes, técnicos de defensa de redes, especialistas en seguridad de redes, operadores de seguridad de redes y cualquier profesional de la seguridad que se encargue de las operaciones de seguridad de redes.

- Analista de ciberseguridad.
- Profesionales de ciberseguridad de nivel básico.

8.2 Programa de formación de nuestro SOC

Paralelamente a las fases de implementación del SOC en nuestra organización, se encuentran las fases de formación del personal. Actualmente no se dispone de un programa de formación con una planificación amplia en el tiempo, porque al igual que el SOC, se encuentra en fase de diseño e implementación, pero al igual que el SOC si que se dispone de una planificación inicial, que consta de lo siguiente:

- Analista nivel 1 (Tier 1): Obtener el certificado CompTIA Security+.
- Analista nivel 2 (Tier 2): Finalizar los estudios de master con este trabajo y obtener el certificado Eccouncil Certified SOC Analyst (CSA).

La idea de planificación es que a lo largo del tiempo los dos analistas de la organización vayan obteniendo más certificaciones que les acrediten totalmente para los servicios básicos que el SOC va a dar a la organización.

9 Conclusiones

La implementación de un SOC en una organización es un reto complejo, que conlleva una planificación a largo plazo, y necesariamente el apoyo de la dirección de la organización. Existen innumerables guías de buenas prácticas y frameworks de trabajo, pero es realmente responsabilidad de la organización decidir cuáles son los servicios que necesita del SOC y aportar los recursos necesarios para llevarlo a cabo. Se ha de entender que es un proceso continuo que no termina una vez el SOC está en funcionamiento, si no que necesita un proceso de mejora continuo y que desde la dirección se interiorice que la seguridad es transversal a toda la organización. Siempre se puede correr el riesgo de pensar que los procesos de negocio de la organización están por encima de la seguridad de la propia organización, pero eso es una política peligrosa que pone en riesgo a los propios procesos de negocio y a la organización en sí misma.

El proceso de implementación descrito en este marco de trabajo, va desde los procesos más esenciales, que es establecer el conocimiento completo de la organización, porque una idea fundamental que nunca hay que olvidar, es que no se puede proteger lo que no se conoce, por ello el primer paso es conocer, conocer los equipos, los servicios, las redes, las configuraciones. Una vez que se conoce en el siguiente paso se ha de identificar, identificar los activos principales, los activos más vulnerables, los que son imprescindibles y de que activos depende estos. Una vez que conocemos e identificamos el siguiente paso es monitorizar, se ha de monitorizar todo lo que se conoce y se ha identificado, para poder estableces patrones de comportamiento normales, si tú tienes un patrón conocido de comportamiento, y cuantos más datos tienes y más conoces más preciso es ese patrón, puedes detectar con mayor facilidad cuando ocurre un hecho anómalo, cuando algo se sale del patrón para poder estudiarlo. Porque hay algo que se ha de tener claro, los hechos anómalos ocurrirán, todas las organizaciones han sido, están siendo y serán atacadas, por ello una organización siempre tiene que estar preparada para este hecho, debe conocer sus puntos débiles y crear planes de contingencia. Cuando ocurre un hecho anómalo se ha de estudiar, para ello se han de disponer de las capacidades y herramientas para su estudio, además de poder responder si realmente se está produciendo un incidente de seguridad. Pero gestionar todos estos datos por analistas humanos no es posible ni mucho menos eficiente, es necesario un mecanismo automático que correlaciones toda la información le dé contexto y significado a los datos aislados para que el analista pueda extraer la información realmente relevante de todo el ruido generado.

Se ha de invertir en formación, los equipos nunca ha de dejar de formarse, es un proceso continuo, tanto al personal del SOC como al de la organización en general, los usuarios es el principal vector de ataque, un click en un link de mail que ha sabido engañar al antivirus y adiós a todas las medidas, ya tienes un incidente de seguridad con un ransomware. Los equipos del SOC deben permanecer en un proceso continuo de formación y mejora, porque es el mundo quien ataca y siempre va a haber alguien muy ingenioso con nuevas e ingeniosas formas de ataque, se ha de estar preparado para todo.

El cómo se implemente realmente el SOC, con que herramientas, dispositivos y equipo dependerá de los recursos que la organización disponga para invertir, aquí es donde surge siempre el problema, porque a las organizaciones cualquier presupuesto en ciberseguridad siempre les parece mucho, y a los responsables de la ciberseguridad siempre tienen la sensación que están infradotados. Y puede que los dos tengan razón, es difícil entender que se ha de invertir en algo que no da resultados ni aporta nada a la cuenta de la organización si funciona bien, porque su trabajo real es ese, que todo funcione bien, es lo que aporta seguridad y continuidad, pero eso son cosas muy etéreas, difíciles de cuantificar, ¿Por qué realmente nos atacarían tanto si no estuviera? ¿realmente serían tan altas las pérdidas que nos compensa tenerlo?, la respuesta a estas preguntas es, nos atacan muchísimo, el peligro es constante, y sí las perdidas serían mucho más altas de lo que se podría proveer. Por eso es lógico que a no ser que existan desde el SOC un proceso constante de concienciación y de formación, es difícil que se valore realmente lo necesario de aportar recursos en seguridad por parte de la organización.

A pesar de la eterna disputa de si los recursos son suficientes o no, lo que está claro, es que siempre se pueden hacer cosas, el SOC de este proyecto se ha implementado completamente con software libre, existe múltiples herramientas disponibles, no es necesario comprar caras herramientas comerciales, aunque está claro que si se dispone de los recursos necesarios seguramente sean la mejor opción, pero existen alternativas para implementaciones con bajo recursos que pueden aportar una gran capa de seguridad a nuestra organización, si se hace bien el trabajo y se siguen las buenas prácticas de forma transversal en nuestra organización.

10 Resultados

Una vez realizado el trabajo toca la parte de presentar los resultados y responder a las preguntas que se nos plantean.

10.1 ¿Qué hemos hecho en este trabajo?

Este trabajo partía de la motivación de ayudar a proteger a las organizaciones, la emergencia sanitaria producida por la covid-19, obligo a las organizaciones en muy breve plazo de tiempo a cambiar su organización, a digitalizar procesos y servicios, esto trajo una mayor exposición a los ciber ataques. En este trabajo se ha intentado crear un marco de trabajo para que una organización implemente un SOC para su protección, a la par que implementábamos uno en la organización para la que trabajo, para que sirviera como referencia práctica, porque sobre la implementación de un SOC, existe mucha información teoría, pero imprecisa y ambigua, esto es debido a la propia naturaleza de un SOC, que depende de la organización que tiene que proteger y de que necesidades tiene que cubrir, además que tiene que aportar servicios, pero no se especifica como o con que tiene que aportarlo. No existen guías o por lo menos durante la realización de este trabajo no las hemos encontrado, que definan prácticamente y de forma definida que pasos se han de seguir para implementarlo. En este trabajo se ha intentado precisamente eso, que alguien lo lea lo siga y encuentre una referencia practica de que hacer, cuáles son los pasos importantes y sobre todo por donde debe comenzar.

10.2 ¿Cómo lo hemos hecho?

El proceso ha sido una mezcla de trabajo teórico y trabajo practico, que se han ido realimentando el uno al otro, se ha investigado en la documentación existente y se han ido dando los primeros pasos, a la vez esos primeros pasos se han implementado prácticamente, dando una visión más amplia a la parte teórica ya que le daba contexto al trabajo, y así se ha continuado a lo largo del trabajo, implementando cada una de las partes y entendiendo cual debería de ser la parte siguiente, porque en el mercado las herramientas existentes definían las funciones prácticas que podíamos realizar y eso ayudaba a centrar la parte teoría del trabajo en cuestiones reales.

Al conocer las partes que componían un SOC, se han buscado herramientas con las que implementarlas y las funciones de las herramientas han orientado el trabajo practico al uso que se le podrían dar y porque, esto a su vez ha ayudado a determinar cuáles eran las siguientes herramientas que teníamos que implementar para cubrir los requisitos que la parte teórica marcaba, y así paso a paso se ha ido realizando el trabajo.

10.3 ¿Qué hemos aprendido? ¿Qué te ha aportado el trabajo?

Pues la verdad es que he aprendido muchas cosas, porque al iniciar el trabajo partía con la idea de que existía un SOC estándar, que existían paquetes de herramientas estándar de un SOC, pero no es así, entonces he aprendido de cada uno de los pasos que se ha dado, para crear un SOC que cumpliera con las necesidades de mi organización. Las herramientas que existían como funcionaban y como se puede implementar un entorno seguro. Ahora tengo una visión mucho más amplia de la ciberseguridad en entornos empresariales y he aprendido un gran número de conceptos sobre buenas prácticas de seguridad en organizaciones.

10.4 ¿Hemos conseguido los objetivos?

Desde mi punto de vista si se han cumplido los objetivos, se dispone de una guía que se puede seguir para implementar un SOC en una organización, que define los pasos y los criterios a seguir. Y se dispone de un SOC implementado como ejemplo para cuya implementación se han seguido los pasos y los criterios de la guía. Facilitando mediante un caso práctico, la comprensión de la teoría.

10.5 Si alguien tuviese que seguir investigando, ¿qué aspectos le propondrías?

Continuar con las siguientes fases de implementación de un SOC, poner un SOC en marcha no es un proceso rápido, no consiste instalar en la organización las herramientas y ya. Lleva un proceso de implementación y uno de puesta en marcha, ese aspecto es el que le propondría que siguiera.

La puesta en marcha de un SOC, la formación del equipo, la obtención de datos y afinación de las reglas para obtener una variable de normalidad lo más precisa posible con la que poder comprar para detectar las anormalidades. LA definición de reglas específicas en los IDS, la puesta en marcha de un plan periódico para el análisis de vulnerabilidades y el descubrimiento de activos, un plan de formación del equipo de SOC y de los empleados de la organización.

11. Glosario

- Aes: Advanced Encryption Standard, también conocido como Rijndael, es un esquema de cifrado por bloques.
- Api: (Aplication program interface) es una interface común entre programas informáticos.
- Auditoría: Proceso sistemático, independiente y documentado para obtener las evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el se cumplen unos criterios fijados.
- Base 64: Es un sistema de numeración posicional que usa 64 como base
- Blowfish: Es un codificador de bloques simétricos
- CSIRT: Equipo de Respuesta a Incidentes de Seguridad Informática, *Computer Security Incident Response Team*.
- Correlacionar: Establecer una correlación o correspondencia entre dos o más cosas.
- DNS: Servicio de nombres de dominio (Domain Name Service).
- Escaner de vulnerabilidades: es un software diseñado para realizar análisis automáticos recogiendo información sobre los servicios en funcionamiento, los puertos abiertos, fallos de configuración y posibles vulnerabilidades conocidas.
- Firewall: un cortafuegos es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado.
- HIDS: Sistema de detección de intrusos en un Host (Host Intrusion Detection System).
- IDS: Sistema de detección de intrusos (Intrusion Detection System).
- IPS: Sistema de prevención de intrusos (Intrusion Prevention System).
- JSON: Formato de texto ligero para el intercambio de datos. (Java Script Object Notation).
- Malware: Software de carácter malicioso cuyo objetivo principal es dañar o infiltrarse en un sistema.
- NIDS: Sistema de detección de intrusos en Red (Network Intrusion Detection System).

- PBKDF: Funcion de derivación clave con un costo computacional variable, que se utilizan para reducir las vulnerabilidades de los ataques de fuerza bruta
- SIEM: Gestión de eventos e información de seguridad (Security Information and Even Management)
- SOC: Centro de operaciones de seguridad (Security Operation Center)
- TCP/IP: Protocolos de transmisión de paquetes
- URL: Localizador de recursos uniforme (Uniform Recource Locator)
- Vulnerabilidad: Debilidad que puede ser aprovechada por una amenaza.

12 Bibliografía

- Security Operations Best Practices, de Christopher J Brown, lulu.com (17 junio 2019).
- Consideraciones para la implementacion de un Centro de Operaciones de Seguridad (SOC): Guía de los aspectos fundamentales de un diseño de SOC, Patricio Campos O, B07921YBKP.
- Security Operation Center - Research on effectiveness of Data Driven SOC, Saifulnizam Sarif, B08PDF9FWR.
- HOW TO SETUP UP CSIRT AND SOC, GOOD PRACTICE GUIDE, DECEMBER 2020, ISBN 978-92-9204-410-7 - DOI 10.2824/056764
- GUIDE FOR CYBERSECURITY EVENT RECOVERY, NIST SP 800-184.
- Ten Strategies of a World-Class Cybersecurity Operations Center, Carson Zimmerman, ISBN 978-0-692-24310-7.
- Guía Del Técnico Para Establecer Un Centro De Operaciones De Seguridad, alienvault technical white paper.
- Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey, Chris Crowley y John Pescatore, July 2019.
- Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology, April 16, 2018
- Computer Security Incident Response Team (CSIRT), Services Framework, Version 2.1.