UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Creación de un SOC para organismo públicos con SIEM

Trabajo Fin de Máster

Máster Universitario en Ciberseguridad y Ciberinteligencia

AUTOR/A: Maqueda Prats, Rubén

Tutor/a: Esteve Domingo, Manuel

CURSO ACADÉMICO: 2022/2023

Resumen.

Este trabajo no solo trata sobre aspectos técnicos de la implantación de un SIEM y comprobación del mismo. Si no que, plantea con una cierta experiencia laboral y profesional abrir y explorar nuevos campos y posibilidades en este "nuevo" y reciente mundo de la ciberseguridad.

Lo normal y común en la sociedad es terminar un plan de formación y buscar trabajo para una empresa. Una vez experimentado este camino durante algunos años y observando las necesidades de ciberseguridad de la mayoría de las empresas, hace replantearse junto a varios compañeros del sector el intentar montar una empresa ofreciendo un servicio de ciberseguridad.

Una vez juntados los cuatro profesionales se decide aprovechar la nueva ley de las start-up. Esto implica que a partir de una persona con un capital de tres mil euros puede formar una sociedad limitada para ofrecer un servicio. La idea es constituir un SOC, centro de operaciones de ciberseguridad, orientando el servicio hacia organismos públicos, aunque sin descartar el mercado privado.

En este punto se estudia que es un SOC, objetivos, organización…Una breve descripción de lo que esto significa. A partir de aquí, se pondrá un ejemplo de contrato a la administración pública, se estudiará normativa a cumplir por el ENS y como unirnse a la red nacional de SOC.

Una vez revisada toda la normativa y contemplado el ejemplo de contrato de un ayuntamiento, se revisará requisitos hardware, de red y presupuestos económicos para ver si es solvente la propuesta o por el contrario no.

Así mismo se adentrará en el aspecto técnico del trabajo. Se propondrá soluciones open-source para ajustarse en el presupuesto económico. Se evaluará la herramienta de gestión de incidentes LUCIA, el SIEM AlienVault y sobre todo el SIEM Onion Security que va a ser la principal herramienta de trabajo. Se implementará estas soluciones y se comprobarará su eficacia, terminando este trabajo en unas satisfactorias conclusiones.

Palabras Clave.

A continuación, se va a exponer siete palabras clave que serán las más usadas en este trabajo para facilitar su lectura y comprensión.

- SIEM (Security Information And Event Management). Sistema de gestión de información y eventos de seguridad.
- SOC **(**Security Operation Center). Centro de seguridad informática.
- CCN. Centro criptológico nacional.
- RT/RTIR (Request Tracker Incident Response). Sistema de gestión de incidentes.
- OSSIM (Open Source Security Information Management). Herramientas open source de seguridad de la información.
- ENS. Esquema Nacional de Seguridad.
- IOC (Indicator of compromise). Indicador de compromiso.

Tabla de contenido.

1. Introducción.

En este primer capítulo, se va a introducir las consecuencias de Internet y digitalización de las empresas e industrias. Se quiere explicar lo que significa estar conectado a esta inmensa red y los problemas que ello conlleva.

Hoy en día la conectividad por parte de una empresa es casi "mandatory" para mejorar eficiencia, prestación de servicios y expansión de negocio. Yendo más allá, la industria también se ha modernizado en una industria conectada conocida como industria 4.0. Las consecuencias de sufrir un ataque en un industria o infraestructura crítica pueden tener consecuencias fatales, desde tener una fábrica cerrada meses con las consecuentes pérdidas económicas hasta su posible cierre.

Hay que tener una conciencia ciber situacional de lo que está pasando en la red, es decir, hay que saber que está sucediendo en la red de una empresa en todo momento usando herramientas para ello.

Para ello, se plantea la "casi" obligada existencia de la implantación o contratación de un centro de operaciones de seguridad que llevará a cabo todas las tareas que se necesita para monitorizar una red, detectar todo tipo de incidentes de seguridad y contener todo tipo de amenazas.

Cuanto más esté "afinado" el SOC más incidentes detectará. El problema más alarmante, es el de sufrir algún tipo de ataque avanzado, el cual podría representar aproximadamente hasta el 5% de los incidentes al cabo del año. Aun siendo un porcentaje bajo, el alto impacto en la organización suele ser grave.

Con ello se quiere explicar que, aunque el software detecte las reglas que se le solicite que detecte, para tipos de ataques modernos y sofisticados lo más probable es que se sufra un ataque si no hay anticipación

1.1 Presentación del problema.

En la actualidad, desde un simple usuario hasta una gran empresa se encuentran expuestas diariamente a las amenazas que circulan por Internet a todo tipo de ataques con intenciones maliciosas y con diferentes objetivos.

Cualquier amenaza de seguridad puede provenir tanto de fuentes internas como de externas. Una preocupación que crece es la posibilidad de que accidentalmente, los empleados estén expuestos a múltiples ataques sin que ellos lo sepan debido a una falta de ciber concienciación y formación. Para prevenir estos problemas, las empresas están incorporando varios sistemas para protegerse de intrusiones y de una gran cantidad de amenazas diversas tales como antivirus, EDR, IPS, firewalls…etc.

La desventaja de estos sistemas de protección es que generan tanta información para monitorizar, que los equipos informáticos se enfrentan al problema de tener que interpretarla en su totalidad para poder reconocer los problemas reales. De hecho, el volumen de datos de seguridad que fluyen a los equipos destinados a ello con poco personal es de poca utilidad. La mayoría de los incidentes pueden ser alertados, pero no procesados por el analista debido a este alto volumen de información. Es aquí donde entra a jugar los sistemas de gestión de información y eventos de seguridad (SIEM).

Los profesionales de ciberseguridad de un SOC se benefician de un sistema de monitoreo en tiempo real siendo fácil de usar. Este sistema es proporcionado por un SIEM, lo que les permite centralizar la gestión de todos los eventos de la red.

Los ataques informáticos han aumentado exponencialmente en la última década. Esto ha provocado que incluso pequeñas empresas con poco personal implementen un SOC como solución principal para monitorear su red [1].

1.2 Antecedentes y justificación.

El acrónimo en inglés SIEM corresponde a Security Information and Event Management, un sistema de gestión de eventos y seguridad de la información que proporciona un denominador común para la recopilación de información.

El 80% de las empresas son víctimas de una avalancha de correos electrónicos maliciosos y múltiples tipos de intentos de intrusión en sus redes corporativas. Evidentemente, el usuario es el eslabón más débil de la cadena de seguridad informática y mediante la ingeniería social un atacante intentará "engañarlo" enviándole correos electrónicos con enlaces y archivos adjuntos maliciosos.

Tanto para usuarios privados como para empresas, el correo electrónico se usa mucho en el trabajo diario y es una herramienta muy importante. Un método de comunicación rápido, seguro y accesible desde cualquier dispositivo y en cualquier lugar. En la actualidad el correo electrónico es el vector de entrada principal desde el punto de mira para los atacantes, un 80% de los ataques es por correo electrónico.

Es una realidad que los datos e información tienen un gran valor hoy en día y son vendidos a terceros para todo tipo de fines. Sin duda uno de los métodos que más utilizan para recopilar direcciones de e-mail son los bots, encargados de buscar en mensajes públicos en todo tipo de redes sociales. Se compromete la privacidad en la mayoría de los casos usando de este tipo de redes donde se expone información para el atacante.

Un SOC permitirá blindar a la organización o industria, un escudo frente a las amenazas y gestión de ellas. Se valorará todas las herramientas necesarias para el correcto funcionamiento, cualificación necesaria del personal, calidad del servicio que se va a ofrecer y presupuesto económico.

Por todo ello, el motor principal del SOC será el SIEM para monitorizar todo tipo de amenazas externas, sin olvidar tampoco diversas herramientas como de respuesta de incidentes, aplicaciones, SOAR, machine learning…etc.

1.3 Hipótesis y objetivos del trabajo.

Este documento describe el proceso de implementación de un SOC. El SOC estará listo para atender a los sectores público y privado. Para ello, se dotarán de herramientas compatibles con los sectores público y privado, de acuerdo con lo previsto en el Plan Nacional de Seguridad de España. Los objetivos que persigue la solución propuesta son:

La realidad de necesitar un SOC, con una plataforma SIEM para monitorear la información de la DMZ o zona desmilitarizada. La plataforma SIEM proporcionaría un centro de control integrado que monitorea los datos. Se destacan más funciones:

- La gestión de amenazas en tiempo real es esencial.
- Generación de informes.
- La red cuenta con sistemas automatizados para responder a eventos sospechosos o amenazas determinadas.
- Los riesgos adicionales que se deben tener en cuenta al evaluar la seguridad de la información incluyen la detección de fraudes en tiempo real, las amenazas internas y externas...etc. Al mitigar estos riesgos, se puede comprender mejor las implicaciones de cualquier problema potencial.
- Una plataforma integrada con un centro centralizado permite el análisis, el almacenamiento y el acceso de datos en tiempo real durante meses. Esto hace posible recopilar información pertinente que puede utilizarse para futuros exámenes forenses.
- Proporcionar una plataforma de respuestas de incidentes.

Elevar las capacidades de formación del personal del SOC, potenciando el conocimiento, experiencia y habilidades del equipo humano actual, mediante:

- Adopción de plataformas modernas, comprensibles, estructuradas en cada función y parametrizable en múltiples funciones.
- Enriquecimiento con funciones avanzadas de control, de visibilidad, de programación, de categorización, contextualización de eventos que permiten explotar al máximo el ingenio en el uso del SIEM.
- Se verán posibles funcionalidades SOAR para respuestas automáticas a incidentes sin intervención humana.

Se contará con múltiples herramientas como Honeypot, Sinkhole, XDR, herramientas sandboxing, SOAR, escáner de vulnerabilidades, machine learning y todas las herramientas complementarias sin llegar a saturar por exceso.

1.4. Organización del capítulo.

Este capítulo trata de introducir la problemática de la transformación digital de las pymes y de la industria, los riesgos que existen de estar conectado y a lo que se está expuesto.

Se expone de cómo la implantación de un centro de operaciones de seguridad puede aportar a una organización o industria un control de lo que está pasando en su red. A su vez, se ve los objetivos que tiene un SOC, para lo que está diseñado, lo que puede prevenir y aportar.

2. Estado del arte.

El presente documento describe la implementación e integración de un SOC con herramientas open source. Que este documento pueda servir en parte de ayuda o pequeña guía para analistas con experiencia que decidan dar el paso a formar un SOC y estar abiertos a prestar servicio a organismos públicos nacionales o al sector privado con casi las mismas herramientas de software, siempre siguiendo la normativa establecida.

2.1 Definición de un SOC.

El acrónimo SOC en español significa centro de operaciones de seguridad, que es un equipo de ciberseguridad. El SOC se enfoca en prevenir el robo de información, detectar ataques y cualquier otro problema de seguridad en una organización.

Las pequeñas empresas lentamente contemplan el valor de contratar un SOC. La misión de un centro de operaciones de seguridad es rastrear vulnerabilidades, actualizar equipos y sistemas, prevenir la entrada de malware…etc. Su misión es maximizar la seguridad para las empresas y organizaciones que desean mantener sus sistemas seguros.

Algunas amenazas pueden poner de rodillas a una empresa en segundos. Por ejemplo, un ataque de ransomware que encripta todos los archivos, un ataque DDoS que cierra los servicios durante horas, robo de información para su posterior venta y malware que provoca fallos en el sistema [2].

2.2 Objetivos de un SOC.

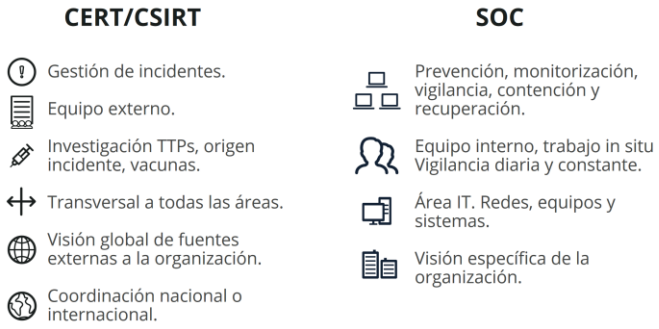
El Centro de Operaciones de Seguridad presenta un enfoque en la mejora de la ciberseguridad para empresas e industrias. Sus principales objetivos son los siguientes:

- Monitorizar los sistemas de información, redes y comunicaciones de la empresa para detectar posibles amenazas.
- Analizar amenazas o ataques para comprender las nuevas armas utilizadas por los ciberdelincuentes y desarrollar herramientas de protección adecuadas.
- Recuperar dispositivos o información perdida dañada por piratería o malware.

- Establecer mecanismos que permitan a las empresas responder de forma más rápida y eficaz a cualquier ataque.

Aparte, el SOC será responsable de verificar el correcto funcionamiento de las siguientes partes relacionadas con la seguridad corporativa: [3]

- Mecanismos de seguridad física.
- Directivas de seguridad y acceso (políticas, procedimientos, etc.).
- Equipos de seguridad perimetral.
- Segmentación de redes.
- "Hardening" de equipos.
- Gestión de aplicaciones y usuarios.
- Encriptación de datos.
- Copias de seguridad.



Cert vs SOC

SOC

2.3 Organización de un SOC.

Para su correcto funcionamiento el SOC se organiza en varios niveles, se ve a continuación:

TIER Nivel 1: En este nivel se encuentran los analistas de alertas de primer nivel, el primer eslabón, son los encargados de detectar e investigar las amenazas que recibe la empresa. Su función es analizar cualquier riesgo de seguridad y según los estándares del SOC, si su riesgo es alto se envían al siguiente nivel.

TIER Nivel 2: Si la amenaza es capaz de causar serios problemas de seguridad, este nivel analiza el posible daño o el sistema afectado. Con base en esta evaluación, se propone una solución a la amenaza.

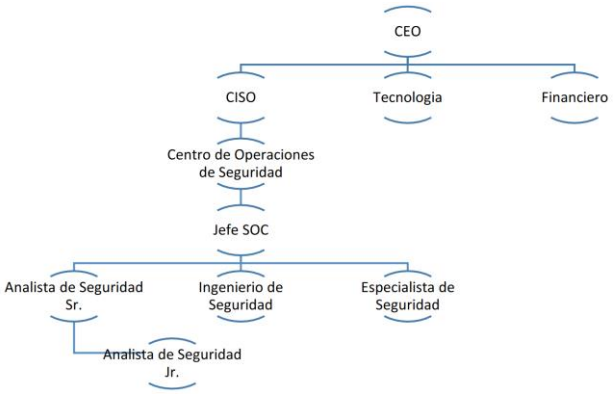
TIER Nivel 3: Este último nivel está formado por profesionales de ciberseguridad con la más alta cualificación. Ellos son los encargados en última instancia de resolver los incidentes de seguridad muy complejos y establecer medidas preventivas para que no vuelvan a producirse [3].

Aparte se tendrá al CISO y al CIO o CEO del SOC. En estos niveles el personal englobado estará constituido por todo tipo de especialista informático como: analistas de ciberseguridad, ingenieros de seguridad, analistas de ciber inteligencia, cazadores de amenazas …etc. Desde los niveles 1 al 3 se trabajará conjuntamente para dar una mejor respuesta de incidentes.

Cada rol tendrá sus funciones y estarán definidas en su correspondiente TIER, aunque dependerán del nivel de formación y experiencia. Se recalca que todos pueden trabajar conjuntamente para mejorar la respuesta ante incidentes.

Organización de un SOC

Ejemplo de jerarquía en un SOC:



Jerarquía del SOC

2.4 Beneficios de un SOC.

A continuación, se verá cómo los SOC benefician a las organizaciones con lo siguiente:

- Un sistema de detección de amenazas en tiempo real es más efectivo cuando el monitoreo se realiza desde una herramienta centralizada.
- Es posible responder instantáneamente a un incidente, a veces inmediatamente después de su descubrimiento gracias al monitoreo constante.
- Al analizar todos los posibles puntos de entrada a un sistema, un SOC puede determinar varios puntos débiles en las redes o la infraestructura de la organización.
- Los equipos de seguridad pueden usar la inteligencia de amenazas para determinar qué amenazas son reales y cuáles no. Esto les permite formular respuestas y estrategias apropiadas a diferentes amenazas.
- Un SOC diario proporciona información detallada sobre los datos de seguridad que facilita la investigación de cualquier incidente que ocurra.
- Contratar un equipo de expertos le permite controlar sus sistemas y redes a largo plazo. Hacerlo es más económico que otras alternativas.

Hay dos categorías principales de centros de operaciones de seguridad, así como una opción híbrida que se adapta a ciertas necesidades. Algunas organizaciones pueden preferir usar una opción híbrida en lugar de un tipo específico. Por ejemplo, un híbrido podría ser más adecuado para organizaciones con requisitos de presupuesto estrictos o restricciones de hardware y software.

2.5 SOC como servicio (SOCaaS). Ventajas e inconvenientes.

Hay dos formas para que una empresa cree un SOC: contratando uno o construyendo uno desde cero. Al tomar esta decisión, es mejor considerar cada caso individualmente. Inicialmente, puede parecer una buena idea que las empresas mantengan sus archivos de registro internamente. Sin embargo, la subcontratación de ciertos servicios tiende a ser más ventajosa. Las razones por las que subcontratar a una empresa especializada son generalmente porque:

1. Las empresas que no cuentan con departamentos de ciberseguridad tienen dificultades para encontrar personal idóneo para este puesto.
2. Es importante que los analistas de SOC se centren exclusivamente en la ciberseguridad. Si se la aparta de su trabajo para realizar otras tareas, pueden descuidar sus responsabilidades principales y pasar por alto brechas de seguridad vitales. Los profesionales de ciberseguridad deberían estar constantemente actualizados y certificados. Este aspecto puede resultar complicado si la empresa no se dedica a la ciberseguridad y si no se cumple, aunque se consiga contratar a los mejores profesionales, su eficacia disminuirá con el tiempo.
3. Un centro de operaciones de seguridad externo monitorea constantemente diferentes empresas y entornos. Trabajar con una sola empresa limita el aprendizaje de amenazas, un SOC externo brinda a los analistas más oportunidades para aprender.

Es importante tener en cuenta que solo el 10% de los ataques cibernéticos no se pueden mitigar con las técnicas SOC tradicionales. Estas técnicas incluyen bloqueo, monitoreo y gestión de vulnerabilidades. En consecuencia, el 48% de los profesionales de la seguridad considera que estos ataques son la mayor preocupación.

Los mejores SOC logran más efectividad a través de una combinación de herramientas avanzadas capaces de correlacionar eventos que a priori pueden parecer independientes y nada peligrosos y un equipo experimentado capaz de interpretar la verdadera escala de estos eventos y mitigar tales ataques [5].

Una ventaja de tener un SOC externo como servicio contratado es que puede omitir la fase de contratación y capacitación y obtener experiencia inmediata que no requiere mucho tiempo de implementación. Estos equipos también mantienen herramientas y soluciones de seguridad integradas y administradas y son competentes en su uso, lo que simplifica aún más los plazos de implementación.

Los equipos de SOC externos también son más escalables, ya que tienen experiencia y están altamente especializados. Por lo general, ofrecen monitoreo las 24 horas los 7 días de la semana, pueden rastrear el panorama actual de amenazas e innovar al mismo ritmo que lo hacen los atacantes. [4].

Por lo tanto, para las organizaciones con experiencia interna y presupuestos de inversión limitados que desean una incorporación rápida para acelerar los resultados, una opción de SOCaaS puede satisfacer sus necesidades.

Como desventajas:

Cobertura integral: los proveedores de SOCaaS a menudo no cubren el espectro completo de necesidades de seguridad, incluida la respuesta a incidentes y el cumplimiento normativo.

Herramientas de seguridad existentes: la mayoría de los proveedores de servicios tienen su propia cartera de soluciones, ya sea desarrolladas internamente o entregadas a través de socios externos, por lo que es probable que ofrezcan cobertura parcial o nula.

Aunque los proveedores a menudo carecen de la tecnología para proporcionar recomendaciones fáciles de entender, también hay tarifas ocultas y falta de transparencia en la seguridad de sus sistemas [6].

2.6 SOC basado en la nube.

Dado que SOCaaS rara vez ofrece todas estas capacidades, es posible que esta solución se quede corta en la realidad. Se considera lo que sucedería si recibiera numerosas alertas, también lo que sucedería si un ransomware infecta la red...

Una opción de plataforma SOC basada en la nube permite un rango de seguridad completo al conectarse a los sistemas existentes. Esta plataforma permite capacidades de seguridad adicionales que pueden no existir aún en la empresa. Al elegir esta opción, se está manejando una plataforma en lugar de un servicio.

El enfoque de plataforma para la ciberseguridad ofrece mucho más que soluciones prediseñadas de proveedores de SOCaaS. Proporciona IA y automatización para brindar seguridad de alto nivel con:

- Integrando comandos centralizados para cada evento de seguridad.
- Integración simple con sistemas de seguridad y fuentes de datos existentes.
- Capacidad de escalar el hardware en caso de necesitar procesar más eventos por ampliación en la compañía.

Los beneficios adicionales de un enfoque de plataforma basada en la nube incluyen:

- Visibilidad contextual dentro y a través de todos los sistemas.
- Ver qué amenazas son reales y comprender su gravedad.
- Ayudar a priorizar actividades relacionadas con incidentes de seguridad.

2.7 SOC interno. Ventajas e inconvenientes.

Muchas organizaciones prefieren mantener su equipo de operaciones de seguridad internamente en lugar de subcontratarlo a un tercero. Es probable que la razón principal de esto sea que no se sienten cómodos confiando la integridad de su red, sistemas y servicios a terceros. En cambio, prefieren confiar aspectos importantes de su negocio a su equipo interno.

Todos los datos relacionados con la actividad, la inteligencia de amenazas y los registros de eventos se almacenan dentro de la organización, lo que significa un mayor control sobre sus activos y menos posibilidades de pérdida de datos. La organización también tiene la ventaja de pasar por alto las soluciones, las herramientas y las políticas de seguridad de las herramientas externas al adaptarlas para que se ajusten a su propia arquitectura. [4].

Construir algo desde cero, como un equipo de expertos en seguridad internos, conlleva costos significativos. Se necesitaría contratar a más personas, esto disminuiría el tamaño de otros departamentos y aumentaría las demandas de contratación de otros departamentos.

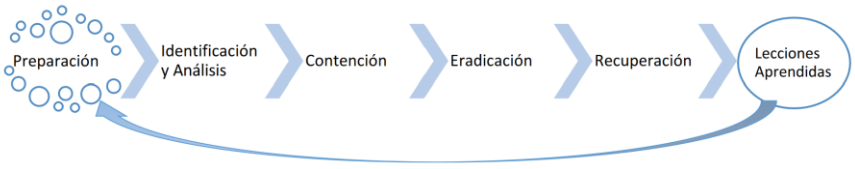
Los empleados que aprenden nuevos conocimientos en ciberseguridad requieren mucho tiempo y dinero para aprender. Una vez que hayan aprendido las nuevas habilidades, estos empleados también necesitarán capacitación para sus nuevos roles.

Los sistemas y herramientas de seguridad de diferentes fuentes rara vez interactúan entre sí. En consecuencia, el uso de muchas herramientas y sistemas diferentes en un departamento de seguridad puede hacer que las tareas tarden más en completarse. [4].

2.8 Normativa.

Para proteger su principal activo, la información de la empresa, se debe implementar un sistema de seguridad. Lo más usual es cumplir ciertos estándares como ISO 17799. Este estándar describe cómo proteger la información de la empresa de posibles amenazas. Abordará conceptos tales como confidencialidad, integridad, disponibilidad, autenticidad, confiabilidad y responsabilidad, sin descuidar la responsabilidad y el repudio.

En los Estados Unidos, es común que los esquemas de gestión de incidentes utilicen el modelo NIST.SP.800.61rev2. Sin embargo, otras organizaciones pueden personalizar su propio esquema.



NIST.SP.800.61rev2

El estándar NIST.SP.800 utiliza tablas con categorías predefinidas para facilitar la evaluación de incidentes. Especifica categorías predefinidas para evaluar los informes de incidentes. Cualquiera que envíe un informe de incidentes en este estándar puede usar una tabla para categorizar cada incidente en función de múltiples factores.

El SOC también puede implementar sugerencias de las normas ISO 27000 y 27001/2 que contienen recomendaciones para la implementación del personal del SOC para mejorar el nivel de seguridad de la información dentro de la empresa. El Esquema Nacional de Seguridad enmarca las medidas de seguridad en la guía 825 del CCN-STIC. Cualquier iniciativa para crear una estructura similar a la propuesta debe tomar como referencia el ENS para implementar sus medidas.

Cualquier iniciativa para crear tal estructura debe ir acompañada de un proceso de implementación del Plan Nacional de Seguridad (ENS) como marco de referencia de las medidas de seguridad a emplear, como se verá más adelante en la CCN-STIC 825. Reportar un incidente ayuda a todos los involucrados, ya que se debe considerar:

- Los incidentes deben clasificarse según el origen de la amenaza, los usuarios afectados, los sistemas afectados y la gravedad.

- Hay cinco niveles de peligro relacionados con los incidentes cibernéticos: alto, muy alto, alto, medio y bajo. Puede encontrar estos niveles clasificados detallados aquí:
- El CCN-CERT gestiona las incidencias prioritarias.
- La Guía CCN-STIC 817.
- El impacto del incidente cibernético se califica como bajo, medio y alto, siendo el daño muy grave la calificación más alta.
- Reportar las causas del incidente cibernético.
- Además de informar al equipo del CCN-CERT sobre incidencias en su departamento, los funcionarios públicos están obligados a informar de determinadas infracciones.
- El CCN-CERT exige el conocimiento de determinadas incidencias.
- El Real Decreto 3/2010 de 8 de enero de 2010 contiene los artículos 24 y 37 del Esquema Nacional de Seguridad, lo que lo convierte en el regulador oficial.
- Apartado gestión de incidentes de seguridad de la Guía CCN-STIC 403/817.
- CCN-STIC-810. Guía de creación de un CERT/CSIRT.
- El ENS está obligado a aplicar la Ley Orgánica 3/2018 en el tratamiento de datos personales. Esta ley garantiza los derechos digitales y protege los datos personales.
- El Real Decreto-ley 43/2021 de 26 de enero de 2019, amplía el Real Decreto-ley 12/2018 de 7 de septiembre de 2018 sobre la nueva ley aborda la seguridad de las redes y sistemas de información.
- Se seguirán las guías CCN-STIC y como apoyo las del NIST:
    - NIST SP 800-61 “Computer Security Incident Handling Guide”.
    - NIST SP 800-83 “Guide to Malware Incident Prevention and Handling”
    - NIST SP 800-86 “Guide to Integrating Forensic Techniques into Incident Response”.
- IETF/RFCS: Es una comunidad internacional de diseñadores de redes, operadores, fabricantes e investigadores. Se describen los más interesantes:
    - RFC2350 “Expectations for Computer Security Incident Response”.
    - RFC3227 “Guidelines for evidence collection and archiving”.
    - RFC 3067 “Incident Object Description and Exchange Format (IODEF)”.
    - RFC 4765 “The Intrusion Detection Message Exchange Format”.

2.9 Red nacional de SOC.

La estrategia de ciberseguridad de la UE para 2020 indica la necesidad de la creación una red de centros de operaciones de seguridad en toda Europa. Esta necesidad fue atendida en mayo de 2022 a través del Centro Criptológico Nacional. Fue en respuesta a la conclusión de que era necesaria una red nacional de SOC basada en inteligencia artificial [8].

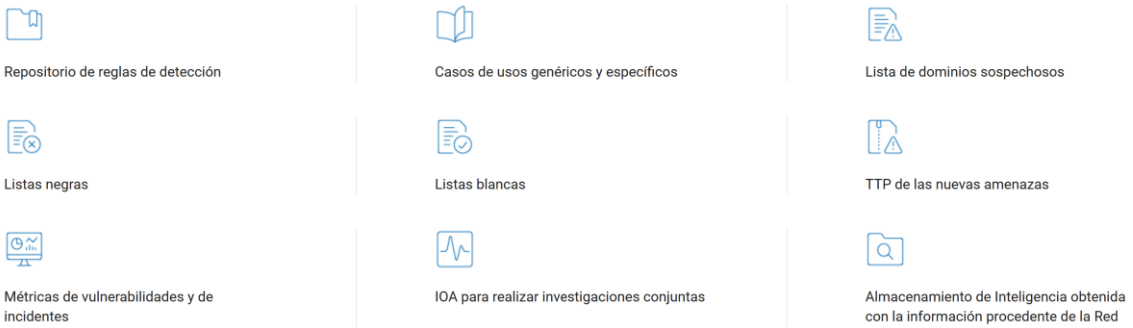
El objetivo del proyecto es facilitar el intercambio de información sobre amenazas tecnológicas entre los SOC del sector público y los proveedores privados que ofrecen este servicio. Esto se hace con el fin de promover la cooperación y el intercambio de información eficiente entre los miembros de la red de SOC nacional, o red de cooperación, que permite a los miembros compartir información técnica en tiempo real. Esto ayuda a los miembros a mejorar sus habilidades de protección y defensa.

Esta red de SOC del sector de servicios públicos reducirá el alcance y la gravedad de posibles incidentes cibernéticos. También mejorará los sistemas de alerta temprana para amenazas potenciales. Así lo demostró el proyecto piloto CCN de enero de 2018 que supuso el primer paso para el despliegue de esta red.

CCN CERT

Capacidades herramientas

Compartir información a través de la red permite a las organizaciones miembro compartir conocimientos sobre amenazas tecnológicas. Este conocimiento compartido se utiliza para mejorar las defensas y las medidas de protección.



Aplicaciones CCN

Herramientas: el CCN-CERT pone a disposición del sector público sus herramientas comunes y compartidas, entre las que destacan:

Herramientas CCN

Diferentes organismos brindan servicios al sector público. Se pueden implementar diferentes SOC de diferentes maneras, algunos sistemas son operados por empleados de la administración pública y otros son operados por proveedores externos.

Esta red es colaborativa y está organizada por categorías y niveles; incorpora agentes tanto públicos como privados. Teniendo que lidiar con el hecho de que algunos centros pueden no utilizar el mismo modelo de gestión, esta red se diseñó para lograr una integración total.

La Red Nacional de SOC contiene organizaciones públicas representadas en una categoría denominada sector público. La categoría privada está compuesta por empresas y proveedores de servicios de ciberseguridad que ofrece un SOC al sector público. Esta categoría privada tiene dos niveles:

Nivel GOLD

- Nivel formado por proveedores que participan de forma activa en la Red.
- La participación en este nivel permite a la empresa recibir indicadores en tiempo real y participar en investigaciones conjuntas.
- Para mantener su posición en esta categoría, se evaluará de forma periódica su participación y colaboración en el intercambio de información.

Nivel INFORMADO

- Nivel de adhesión por defecto de proveedores de servicio a la RNS.
- Recibirá información compartida por los integrantes de la categoría GOLD, una vez consolidada.
- Los proveedores pueden ascender a nivel GOLD si su participación y colaboración es evaluada de forma favorable.

Niveles

Procedimiento y requisitos de adhesión para organismo privado:

Proveedor de servicios

Procedimiento de adhesión:

- ✓ Verificar el cumplimiento de los requisitos generales
- ✓ Solicitar la adhesión a la RNS a través de la dirección: rns@ccn-cert.cni.es
- ✓ Remitir al CCN el formulario de adhesión cumplimentado, que será facilitado al proveedor tras el paso anterior
- ✓ Remitir al CCN el formulario de autorización debidamente cumplimentado

Requisitos mínimos de adhesión

- Ser empresa (pública o privada)
- Prestar servicios de ciberseguridad a la Administración Pública (AGE, Comunidades Autónomas o Entidades Locales)
- Emplear la herramienta LUCÍA del CCN-CERT para la notificación de incidentes
- Aceptación del código ético y de conducta profesional de la RNS
- Autorización firmada de clientes implicados para compartir información no confidencial y anonimizada
- Participación activa en el intercambio de información

Requisitos adhesión

El artículo 11 de la directiva de seguridad de la red de la UE requiere el desarrollo de una red SOC nacional. En consecuencia, el 26 de enero se dictó el RD 43/2021 por el que se ordena al CCN-CERT la creación de una plataforma de seguimiento y notificación de ciber incidentes. Esta plataforma permitirá el intercambio de información entre operadores de servicios esenciales, proveedores de servicios digitales, autoridades pertinentes y CSIRT.

2.10 Esquema nacional de seguridad.

El Real Decreto 311/2022 regula el ENS. En el apartado anterior se vió que los SOC privados tienen que cumplir ciertos requisitos para poder prestar servicios en el sector público.

Al visualizar el certificado de conformidad a través del ENS de la empresa, se puede ver su fecha de renovación más reciente. Además, se puede ver información detallada sobre el artículo certificado por la empresa.

El 3 de mayo, en la hoja de ruta de transición quería que todos los sistemas ya certificados y en proceso de certificación recibieran la certificación del RD 311/2022 antes del 5 de mayo de 2024. El CCN alentó a los organismos certificadores a instar a sus clientes a buscar asesoramiento para evitar el vencimiento de sus certificados. También querían sistemas certificados según el nuevo RD para aumentar la confianza en los sistemas aplicados con certificaciones ENS acreditadas.

Se realiza voluntariamente una auditoría de cumplimiento satisfactoria para recibir la certificación de conformidad ENS de un organismo de certificación acreditado para cualquier sistema de categoría BASICA. Se muestra un ejemplo de certificado:

Cámara Certifica

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría ALTA RD 3/2010

CERTIFICADO DE CONFORMIDAD CON EL ESQUEMA NACIONAL DE SEGURIDAD

CERTIFICACIÓN Y CONFIANZA CÁMARA, S.L.U.

CERTIFICA

Que los sistemas de información reseñados, todos ellos de categoría **ALTA** y los servicios que se relacionan, de

07 GLOBALAN, S.L.

C/ La Marina, 16. 38001. Santa Cruz de Tenerife (Canarias)

han sido auditados y encontrados conforme con las exigencias del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica, según se indica en el correspondiente Informe de Auditoría de 03/04/2022 para:

Los sistemas de información que soportan los servicios de:
- Networking (interconexión de red de datos), los servicios de gestión, explotación y administración asociados.
- Seguridad de los sistemas y de las comunicaciones
- Videovigilancia y control de accesos
- Tratamiento de datos extraídos de las infraestructuras de red desplegadas
- Servicios de mantenimiento y soporte con resolución de incidencias.

Conforme con el documento de categorización del sistema vigente.

Número de Certificado	ENS.3359.22
Fecha de certificación de conformidad inicial	05/07/2022
Fecha de renovación de la certificación de conformidad	05/05/2024

Certificado ENS

2.11 Panorama actual.

Aunque la sociedad avanza a un mundo tecnológico y conectado para expandirse sigue habiendo empresarios reticentes. Cuando al ofrecer los servicios de un SOC pregunten el por qué y para qué quieren gastar parte de sus beneficios en seguridad, la respuesta es sencilla, ante un ataque contundente de un ransomware la empresa puede estar meses parada o incluso entrar en quiebra. Cuando se traslada a pérdidas económicas, osease con números se concienciarán automáticamente de la importancia mostrándole ejemplos reales de otras compañías.

A continuación, se verán noticias para comprobar cómo ha evolucionado el panorama actual de 3 años en adelante:

El 72% de las empresas con SOC lo califican como esencial o muy importante

Endpoint 09 JUL 2020

El presupuesto anual medio de ciberseguridad para las organizaciones ha aumentado en un año de 6 a 31 millones de dólares, con el SOC representando más de un tercio de ese total. El 60% de los miembros del SOC está considerando cambiar de carrera o dejar su trabajo debido al estrés.

El 82% de los SOC confía en su capacidad para detectar ciberamenazas

Endpoint 22 JUN 2020

Mientras que los líderes de los SOC creen que las vulnerabilidades de phishing y de la cadena de suministro son los problemas más importantes, los analistas ven los ataques DDoS y el ransomware como las mayores amenazas. Se espera que las herramientas SOAR tengan prioridad.

Más de la mitad de las organizaciones disponen de un SOC interno

Endpoint 02 DIC 2019

Un 88% de las empresas cree que la automatización ha mejorado las habilidades técnicas de su personal y el conocimiento general de la ciberseguridad. El 61% utilizan una plataforma de inteligencia de amenazas y el 76% investigan las pistas forenses de los correos electrónicos de phishing.

¿Por qué va a creer el mercado de los SOC como servicio?

Actualidad 22 MAY 2019

Un estudio de MarketsandMarkets apunta que el mercado de los Centros de Operaciones de Seguridad crecerá en la modalidad de servicio en torno al 25% anual. La demanda de los SOC as a Service será mayor por el incremento de los ataques, los cambios en las regulaciones de protección de datos o el aumento de la adopción de soluicones cloud por parte de las PYMES, entre otros factores.

Las empresas con un SOC reducen el coste de un ataque en más de la mitad

Endpoint 03 OCT 2019

En cambio, externalizar la seguridad a un proveedor de servicios gestionados (MSP) puede aumentar el impacto financiero, especialmente si la empresa utiliza uno no cualificado. Otra forma de reducir el coste de una brecha es contratando un Delegado de Protección de Datos (DPO).

La mitad de las empresas están insatisfechas con la efectividad de su SOC

Endpoint 24 ENE 2020

Las organizaciones gastan una media de 2,86 millones de dólares anuales en sus SOCs internos, una cantidad que se eleva a 4,44 millones si las organizaciones subcontratan a un proveedor de servicios de seguridad gestionados. Pese a esta elevada inversión, la mayoría no están satisfechas.

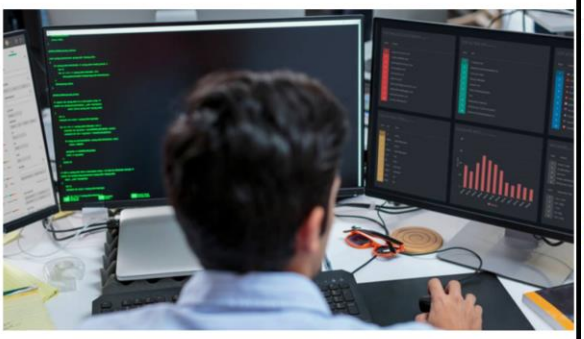
La falta de personal hace que el 70% de los equipos de los SOC estén sobrecargados

Endpoint 28 MAY 2021

El 42% de los responsables de la toma de decisiones de TI y SOC en España cree que su equipo se ve abrumado por el volumen de alertas y el 48% no confía en su capacidad para priorizarlas y responder a ellas. De hecho, éstos dedican hasta un 25% de su tiempo a lidiar con falsos positivos.

4 de cada 10 responsables de seguridad dejarían su puesto por exceso de trabajo

Endpoint 08 MAR 2021



El 80% del personal de seguridad TI en Europa confiesa realizar actividades de ocio durante las horas de trabajo. El 43% señala que sus distracciones en horario laboral se deben a la necesidad de un descanso entre tareas, más que al aburrimiento o a la falta de trabajo.

Muchos SOCs están repletos de herramientas de seguridad redundantes

Endpoint 18 OCT 2021

Las organizaciones no solo tienen que pagar por las licencias y el mantenimiento, sino que los equipos de los SOCs están cada vez más estresados tratando de gestionar múltiples soluciones. El 92% ha considerado los servicios gestionados para externalizar sus capacidades de detección y respuesta.

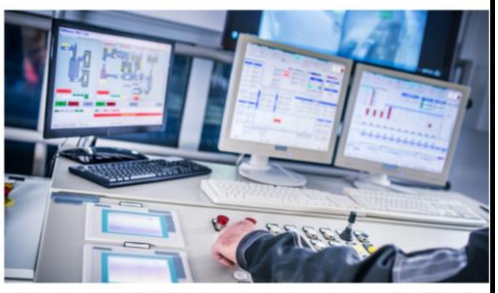
El exceso de alertas 'fatiga' a los analistas de los SOC

Actualidad 10 OCT 2019

Los equipos de ciberseguridad de todo el mundo se enfrentan a un volumen cada vez mayor de alertas de seguridad lo que, unido a la escasez de profesionales en este ámbito y el exceso de tareas que asumen, está provocando lo que se denomina "fatiga de alerta". Esto les impide responder con agilidad y precisión ante los ataques, advierte Cytomic.

Las empresas no están satisfechas con el retorno de la inversión de su SOC

Endpoint 19 ENE 2021



Las organizaciones se enfrentan a una avalancha de crecientes costes de las operaciones de seguridad, pese a lo cual no están satisfechas con su capacidad para combatir las crecientes ciberamenazas. Muchos equipos de seguridad prevén invertir en XDR y automatización de la seguridad.

Resumiendo, se ve que las empresas consideran importante tener un SOC implementado y el disponer de ello reduce costes en caso de incidentes. La mayoría de los SOC se ven capacitados frente a todo tipo de amenazas. Más de la mitad de las empresas disponen de un SOC interno, pero se ve que la línea de modelo será contratarlo como servicio.

Se observa sin embargo que la mitad de las empresas encuestadas no están satisfechas con la efectividad de sus SOC ni con sus retornos de inversión (ROI), lo cual da lugar a la implementación de medidas de automatización.

El problema de los SOC se incentiva con la falta de personal trabajando con gran cantidad de falsos positivos, alrededor de un 45% en el cual se destina un 25% del tiempo y con gran cantidad de herramientas redundantes. Los analistas declaran trabajar con mucha fatiga debido al volumen de alertas y un 40% de responsables dejaría su puesto de trabajo.

2.12 Organización del capítulo.

En este capítulo se ha visto la definición de un centro de operaciones de seguridad, sus objetivos, funciones, como se organiza el personal con diferentes roles y funciones para cada rol y los beneficios que se obtendrá con la implantación de un SOC.

Se ha abordado los tipos de SOC con sus ventajas e inconvenientes tanto internos como externos y basados en la nube.

Se entrará en normativa que servirá de guías como: ISO 27001, NIST, CCN-STIC, se podrá encontrar todo tipo de documentación para el funcionamiento del SOC y también como certificar el SOC para prestar servicios a un organismo público. Se ha comentado también el concepto de la red nacional de SOC con sus ventajas y objetivos.

Se ha mencionado el esquema nacional de seguridad y los requisitos de certificación que se deberá cumplir para prestar servicios a organismos públicos. Finalmente se comenta como está la situación actual de los SOC hoy en día.

3. Metodología de la investigación.

En este capítulo se va a definir las características del SOC, las herramientas de las que se va a disponer, el modelo de empresa que se va a iniciar, personal que debe de constar con diferentes perfiles, roles y demás detalles tanto de negocio como de herramientas implementadas básicas y ampliación en un futuro.

3.1 Modelo de negocio.

El modelo de negocio consistirá en una sociedad limitada aprovechando la nueva ley de los startups. Se observan numerosos beneficios:

- Con este proyecto de ley se incluyen importantes rebajas fiscales y procedimientos flexibles para incentivar la creación e inversión en nuevas empresas de base tecnológica como startups.
- La UE otorga exenciones fiscales a trabajadores, inversores y empresas emergentes.
- Todos los formularios se completan en un solo paso a través de un documento digital notariado. Esto elimina la necesidad de notarios o registros.
- Además, el gobierno anuncia una reducción del impuesto de sociedades del 25% al 15% y la implementación de un impuesto sobre la renta para no residentes durante cuatro años.
- Las opciones sobre acciones pasan de una exención fiscal de 12.000 a 50.000 euros al año cuando se utilizan como forma de compensación.
- Con empresas de reciente o nueva creación, se ofrece una base de deducción anual incrementada de 60.000 a 100.000 euros.
- España fomenta la atracción de talento creando un visado especial para familias de empleados, empresarios y nómadas digitales; y creando un régimen fiscal más favorable para los no residentes en España. Esto se debe a que se otorgan ventajas fiscales a los no residentes de 5 años, que pueden acceder a la visa especial. Además, las ventajas fiscales son mejores para aquellos no residentes que tienen al menos 1 hijo en su familia.
- Afiliarse a los beneficios del seguro social agrega otra doble contribución para los empleados que también manejan su propio negocio. Esto se debe a los incentivos gimnásticamente mantenidos por el gobierno federal.

- El FondICO Next Tech fue creado por el gobierno para ayudar a crecer a las nuevas empresas tecnológicas. Ofrece financiación en forma de un préstamo de interés diferido.[13].

Se va acogerse a esta nueva ley para crear la S.L. con las siguientes ventajas:

- Los activos y el capital social pertenecen a la empresa.
- En comparación con una sociedad anónima, la burocracia es más fácil de implementar y administrar.
- Debido al pequeño capital social con un mínimo inicial de 3.000 €, las empresas también pueden utilizar los fondos para financiar inversiones o necesidades de liquidez.
- Una sola persona es el mínimo ampliando a más.
- Cuando ganas más dinero evidentemente pagas más impuestos. Como resultado de las tasas progresivas del impuesto sobre la renta que son superiores a las del registro de sociedades, los impuestos aumentan a medida que aumentan sus ingresos. En consecuencia, a partir de un determinado nivel de ingresos, los impuestos compensan las ventajas de la Tributación de Sociedades. Las ventajas del Impuesto sobre Sociedades sólo se aplican si los beneficios de la empresa permanecen en el patrimonio de la empresa.
- Las personas que trabajan por cuenta propia pueden pagarse las nóminas y reclamarlas como gastos.
- El fácil acceso al crédito bancario brinda un posible crecimiento a las empresas. [14].

3.2 Plataformas elegidas.

Aquí se definen las herramientas a usar y las que se van a implementar en el proyecto. Como se ha comentado anteriormente no se usarán herramientas redundantes para no saturar al personal del SOC.

SIEM: será el motor del SOC y la herramienta de ciber conciencia situacional. A través de panales estadísticos y generación de informes se podrá saber cómo está la “salud” de la red. Para el caso se elegirá la solución open source Onion Security. Es una distribución de Linux gratuita y abierta para la búsqueda de amenazas, la supervisión de la seguridad empresarial y la gestión de registros.

Security Onion no es un SIEM en sí, es un conjunto de herramientas conectadas para tal funcionalidad, incluye una interfaz web nativa con herramientas integradas que los analistas usan para responder a alertas, búsqueda de amenazas, monitorear el rendimiento de la red y muchas más funciones. Se incluyen herramientas de terceros, como Elasticsearch, Logstash, Kibana, Suricata, Zeek (anteriormente conocido como Bro), Wazuh, Stenographer, CyberChef, NetworkMiner y algunas más.

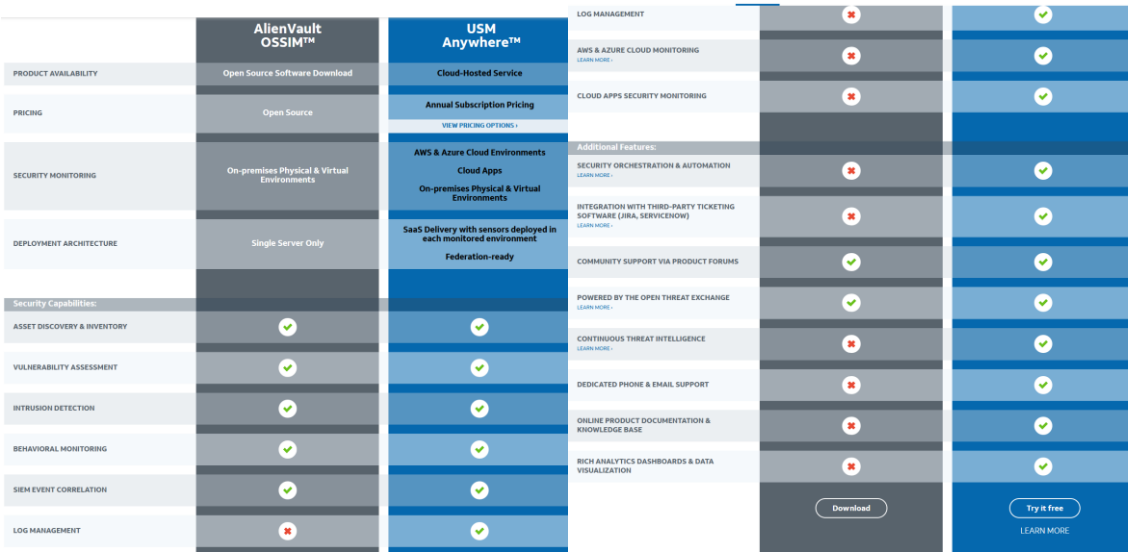
Es altamente escalable, funciona desde un único dispositivo de red hasta una red de mil nodos, las herramientas que se integran están todas abiertas al público, escritas por miembros de la comunidad de seguridad. El código fuente está disponible en GitHub. Cuenta con NIDS (detector de intrusos en la red) recopilando eventos de red de Zeek, Suricata y otras herramientas. Cuenta con HIDS (detector de intrusión en el host) es compatible con varios agentes de recopilación de eventos basados en host como Wazuh, Beats y osquery. También incorpora herramientas de análisis estático (importación de PCAP y EVTX). Incluye soporte para registros de eventos de Windows.

También está disponible una opción de instalación de estación de trabajo para que los analistas de SOC usen herramientas locales de Linux para realizar análisis de eventos de red y host, con lo cual no sería necesario contenedor Docker o subsistemas de Linux bajo Windows.

Como SIEM complementario y en red segura se usará OSSIM de AlienVault, SIEM de código abierto con funciones de recopilación, normalización y correlación de eventos. Proporciona una plataforma unificada con muchas de las capacidades de seguridad esenciales que necesita como:

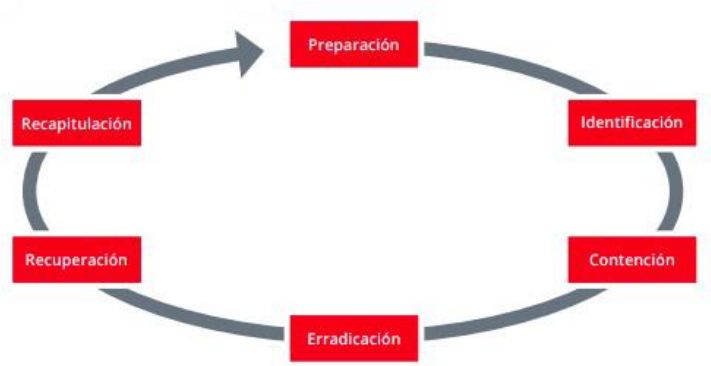
- Descubrimiento de activos.
- Evaluación de vulnerabilidad.
- Detección de intrusos.
- Monitoreo de comportamiento.
- Correlación de eventos SIEM.

Aprovecha la funcionalidad de Open Threat Exchange (OTX) al permitir que los usuarios contribuyan y reciban información en tiempo real sobre IOC maliciosos como plataforma de inteligencia. AlienVault OSSIM ofrece aumentar la visibilidad y el control de la seguridad en su red. Si se requiere más funcionalidad se puede pasar a USM, observando las diferencias y más adelante precios:



Comparación USM vs OSSIM

Gestión de incidentes RTIR (request tracker for incident response): Definido en el RD 43/2021, si el SIEM es el motor del SOC, la plataforma de gestión de incidentes se podría decir que es la transmisión del SOC. Se plasma todo lo que el SIEM recoge a la plataforma de incidentes en caso de serlo. Sirve también como herramienta de ciber conciencia situacional para saber en todo momento que incidentes han sucedido y están en progreso.



Flujo de incidente

Estas serán las fases de la gestión de incidentes:

- Preparación: Se recopilan las herramientas necesarias para el tratamiento del incidente (antimalware, análisis de logs, escáner de vulnerabilidades, back up…etc.
- Identificación: Donde se detecta el incidente, se determina el alcance y se conforma una solución. También conocida como fase de detección y análisis.
- Contención: Impedir que el incidente se extienda a otros recursos, por lo que se minimizará su impacto.

- Erradicación y recuperación: Eliminación de los elementos comprometidos y recuperación planificada del servicio.

Categorización de incidentes:

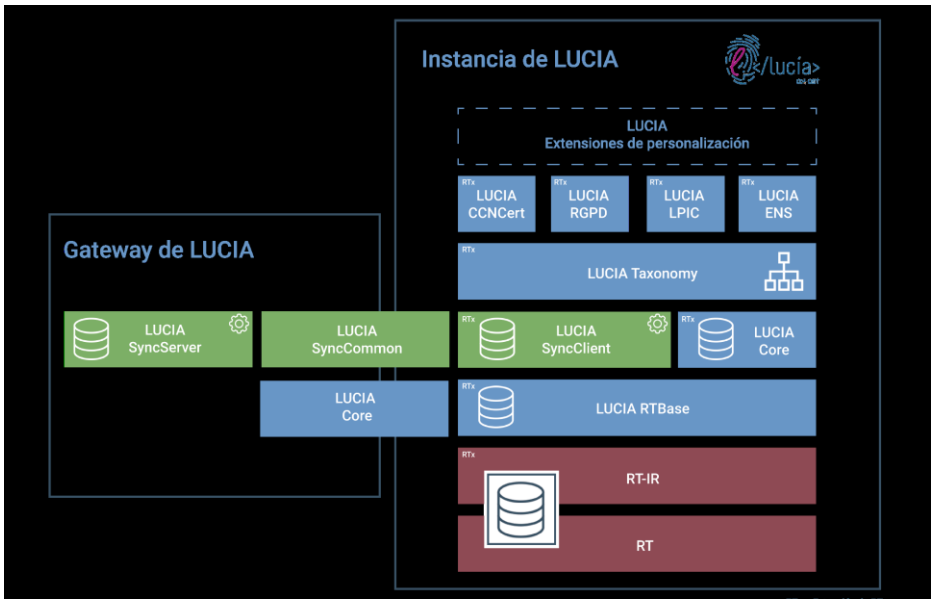
- Naturaleza del incidente.
- La criticidad del/los sistemas/s afectado/s y número de sistemas afectados.
- Impacto que el incidente puede tener en la organización.
- Los requerimientos legales y regulatorios.

La plataforma elegida es LUCIA (Listado Unificado de Coordinación de Incidentes y Amenazas) siendo compatible con sector público. Aparte secanaliza otra open-source. Se procede a analizarla:

- Herramienta de gestión de incidentes basada en el sistema Request Tracker Incident response.
- Elaborado de acuerdo con la guía de gestión de incidentes 817 del CCN. Además, es personalizable para cumplir con los requisitos del CERT y la ENS.
- Automatización de tareas.
- Arquitectura federada distribuida mediante la información sincronizada y compartida con los diferentes organismos adscritos.

Características:

- Sistema Open Source basado en Centos 7 sin coste de licencias.
- Versiones de virtualización disponible en múltiples plataformas.
- Securización a nivel de sistema operativo y aplicativo mediante el uso de certificados de cliente para el navegador.
- Canal de sincronización cifrado y autenticado con protocolos de comunicación REST sobre HTTPS.
- Actualizaciones de seguridad y versiones distribuidas desde el CCN.
- Totalmente personalizable.



Instancia LUCIA

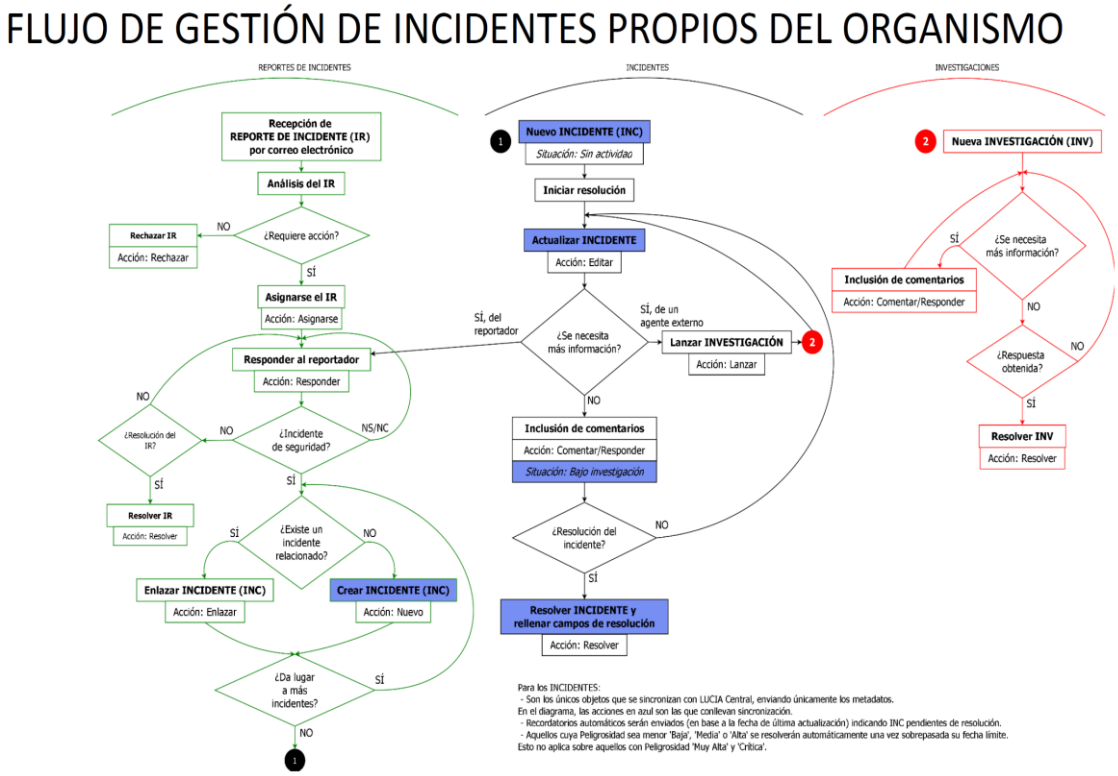
Federación LUCIA

Tickets o casos son la unidad básica de información de LUCIA. Un ticket está formado por:

- Atributos descriptivos que le dotan de metainformación.
- Historial información de contexto.
- Adjuntos.

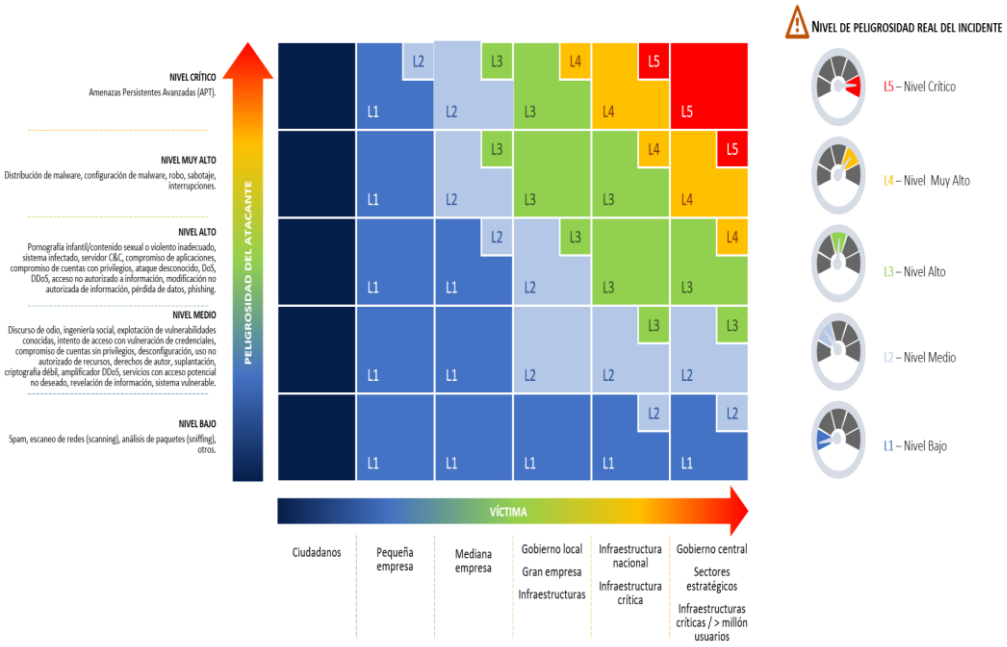
Cola es la unidad organizativa en LUCIA en la que los tickets se dividen en tres tipos

- Reporte de incidentes ó Incident Reports son una comunicación iniciada fuera de LUCIA.
- Investigaciones ó Investigations son una comunicación iniciada desde LUCIA.



Flujo de Gestión de incidentes

Siguiendo la guía STIC 817 de gestión de incidentes es necesario fijar criterios de determinación de peligrosidad de incidentes para así actuar sobre unos u otros y establecer una peligrosidad. A continuación, se muestra una tabla de niveles:



Nivel de peligrosidad

Métricas e indicadores: existe un conjunto de métricas e indicadores que los organismos del ámbito de aplicación del ENS pueden usar para evaluar la implantación, eficacia y eficiencia del proceso de gestión de ciber incidentes. Existen varias métricas como, por ejemplo:

Indicador	Estado de cierre los incidentes	
Objetivo	Ser capaces de gestionar incidentes de seguridad	
Método	Se mide el número de incidentes que han sido cerrados sin respuesta. Fórmula: # incidentes de seguridad cerrados sin	
Caracterización	Objeto	<10%
	Umbral amarillo	20%
	Umbral rojo	50%
	Frecuencia mediación	Trimestral
	Frecuencia reporte	Anual

Indicador	Recursos consumidos	
Objetivo	Conocer si es necesario aumentar la fuerza de trabajo	
Método	Estimación del número de horas-hombre dedicadas a resolver incidentes de seguridad fórmula: #horas dedicadas a incidentes / #horas formalmente contratadas para seguridad TIC	
Caracterización	Objetivo	< 20%
	Umbral amarillo	20%
	Umbral rojo	50%
	Frecuencia medición	trimestral
	Frecuencia reporte	anual

Indicador	Resolución de ciberincidentes de nivel de impacto MEDIO (ENS Anexo I – afectando a sistemas de categoría MEDIA)	
Objetivo	Ser capaces de resolver prontamente incidentes de impacto medio	
Método	Se mide el tiempo que se tarda en resolver un incidente con un impacto en sistemas de categoría MEDIA: desde que se notifica hasta que se resuelve: • T(50) tiempo que se tarda en cerrar el 50% de los incidentes • T(90) tiempo que se tarda en cerrar el 90% de los incidentes	
Caracterización	Objetivo	T(50) = 0 && T(90) = 0
	Umbral amarillo	T(50) > 10d || T(90) > 30d
	Umbral rojo	T(50) > 15d || T(90) > 45d
	Frecuencia medición	anual
	Frecuencia reporte	anual

Indicador	Resolución de ciberincidentes de nivel de impacto ALTO (ENS Anexo I – afectando a sistemas de categoría ALTA)	
Objetivo	Ser capaces de resolver prontamente incidentes de alto impacto	
Método	Se mide el tiempo que se tarda en resolver un incidente con un impacto en sistemas de categoría ALTA: desde que se notifica hasta que se resuelve • T(50) tiempo que se tarda en cerrar el 50% de los incidentes • T(90) tiempo que se tarda en cerrar el 90% de los incidentes	
Caracterización	Objetivo	T(50) = 0 && T(90) = 0
	Umbral amarillo	T(50) > 5d || T(90) > 10d
	Umbral rojo	T(50) > 10d || T(90) > 20d
	Frecuencia medición	anual
	Frecuencia reporte	anual

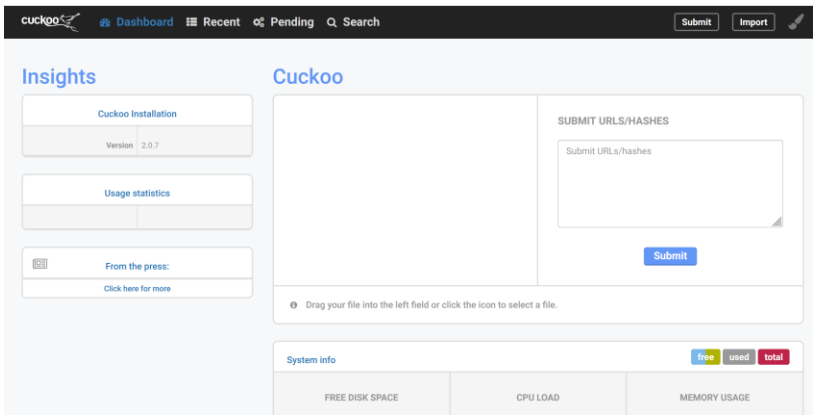
Métricas

Como alternativa hay otra solución open source que es The Hive, plataforma de respuesta a incidentes de seguridad gratuita y de código abierto escalable y diseñada para facilitar la vida de los SOC, CSIRT, CERT y cualquier profesional de la seguridad de la información que se enfrente a incidentes de seguridad que deban investigarse y actuar rápidamente. Su sitio web oficial: https://thehive-project.org. TheHive

Sandbox y análisis de malware.

Para el análisis de malware se usará herramientas manuales como Ghidra o Ida Pro usadas por personal con experiencia para amenazas complejas y poder obtener resultados ampliados, sin embargo, para un análisis rápido y sacar los IOC´s para su bloqueo se usa la herramienta ADA del CCN y la sandbox Cuckoo. Las dos como servicios a través de web: https://sandbox.pikker.ee/ ó https://cuckoo.cert.ee/

Para documentación de uso se puede consultar su web oficial: https://cuckoo.sh/blog/

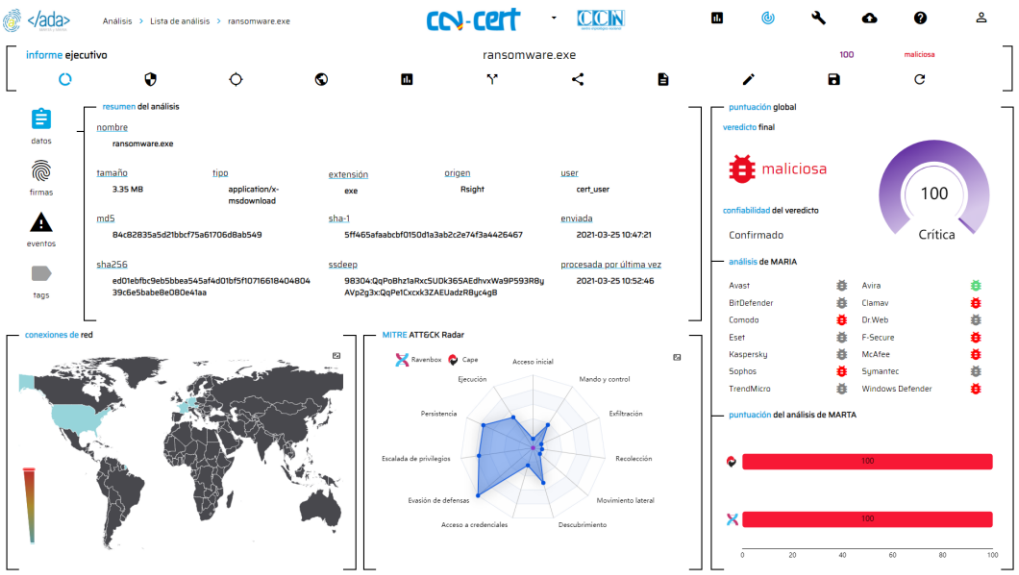


Sandbox Cuckoo

ADA realiza análisis estático y dinámico. Al analizar la muestra binaria aparecerá un informe y una métrica:

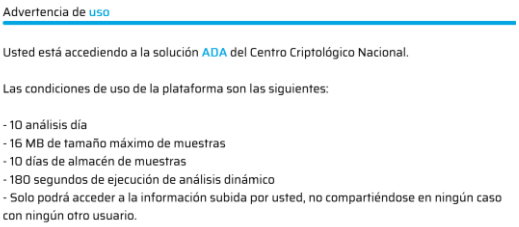
Sandbox ADA

Interfaz de trabajo de ADA:



Interfaz ADA

Tiene ciertas limitaciones que se muestran en las advertencias del uso:


Advertencia de uso

Usted está accediendo a la solución ADA del Centro Criptológico Nacional.

Las condiciones de uso de la plataforma son las siguientes:

- 10 análisis día
- 16 MB de tamaño máximo de muestras
- 10 días de almacén de muestras
- 180 segundos de ejecución de análisis dinámico
- Solo podrá acceder a la información subida por usted, no compartiéndose en ningún caso con ningún otro usuario.

Limitaciones ADA

Aparte al recibir un binario sospechoso, mientras se analiza, se puede sacar su hash y buscarlo en plataformas y también análisis de web:

- https://www.virustotal.com/gui/home/upload
- https://urlscan.io/
- https://any.run/
- https://www.joesandbox.com/
- https://www.hybrid-analysis.com/
- https://www.intezer.com/
- https://sandbox.anlyz.io/
- https://gchq.github.io/CyberChef/
- https://capesandbox.com/

Herramienta de inteligencia. Reyes. 

Tiene como objetivos:

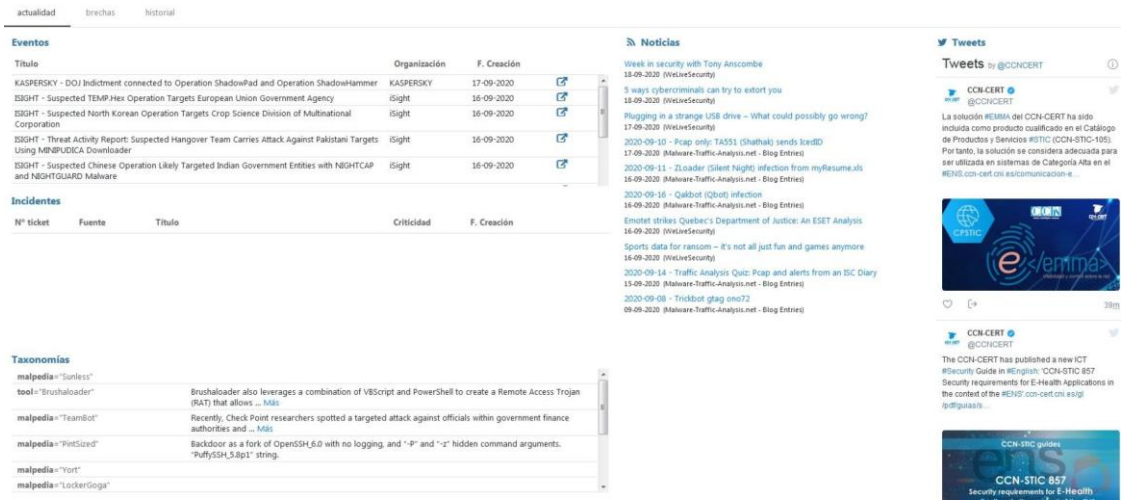
- Recoger información de fuentes públicas y privadas.
- Centralizar en una única plataforma todo el conocimiento.
- Realizar investigaciones de forma rápida y sencilla.
- Relacionar información de las diferentes fuentes.
- Generar inteligencia para los sistemas de seguridad perimetral.

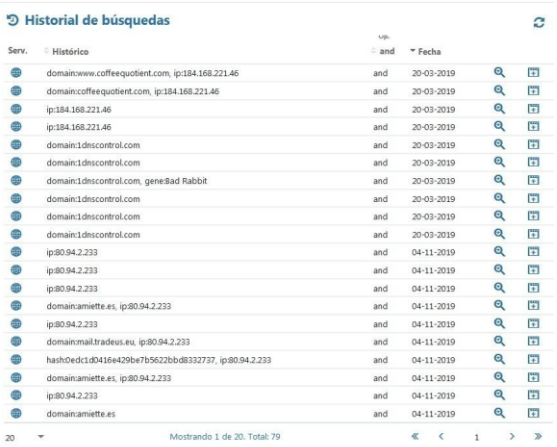
Como características se tiene:

- Inclusión de pestañas de actualidad, brechas, historial, filtros, términos de búsqueda, módulo CIF para las descargas de listas negras y descargas en CSV.
- Interacción del grafo de inteligencia modificando nodos.

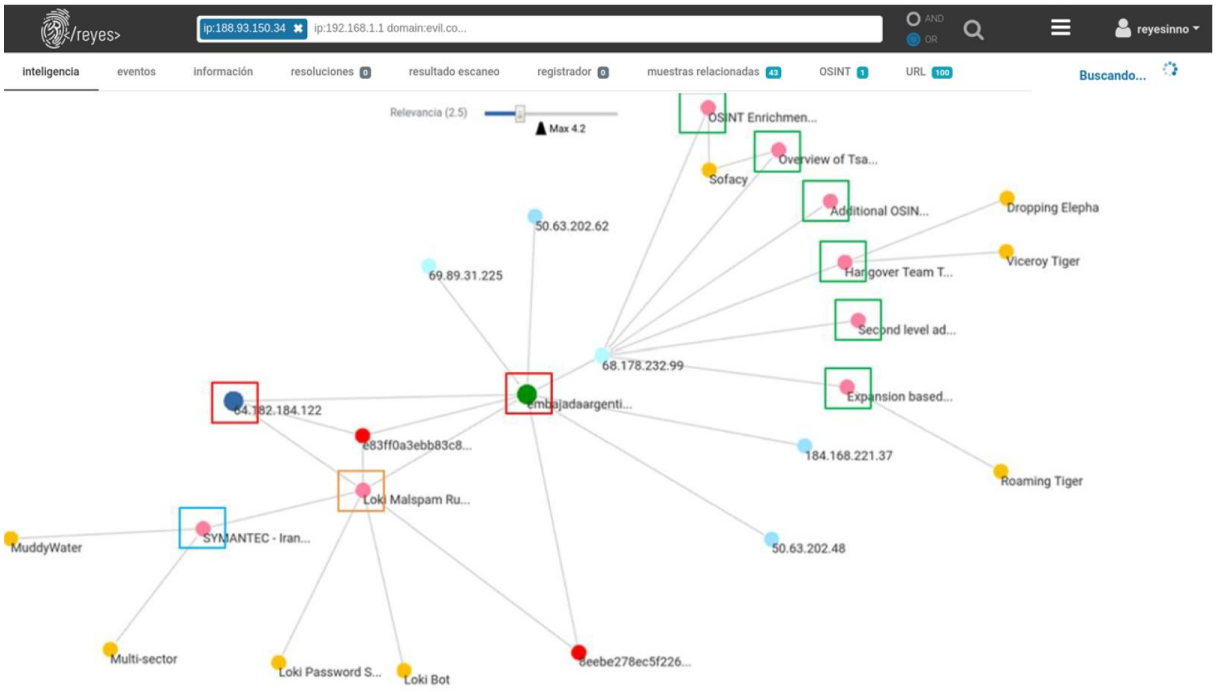
- Investigación e inclusión de nuevas fuentes integrándose con los términos de las búsquedas.
- Permite realizar una investigación de forma rápida y sencilla con configuración de búsquedas.
- Acceso a información exclusiva y restringida.
- Descarga de muestras, informes, reglas e indicadores.
- Ayuda a compartir información de forma controlada.

Aquí se ve la interfaz de la versión 3.0 y 4.0. Reyes 3.0

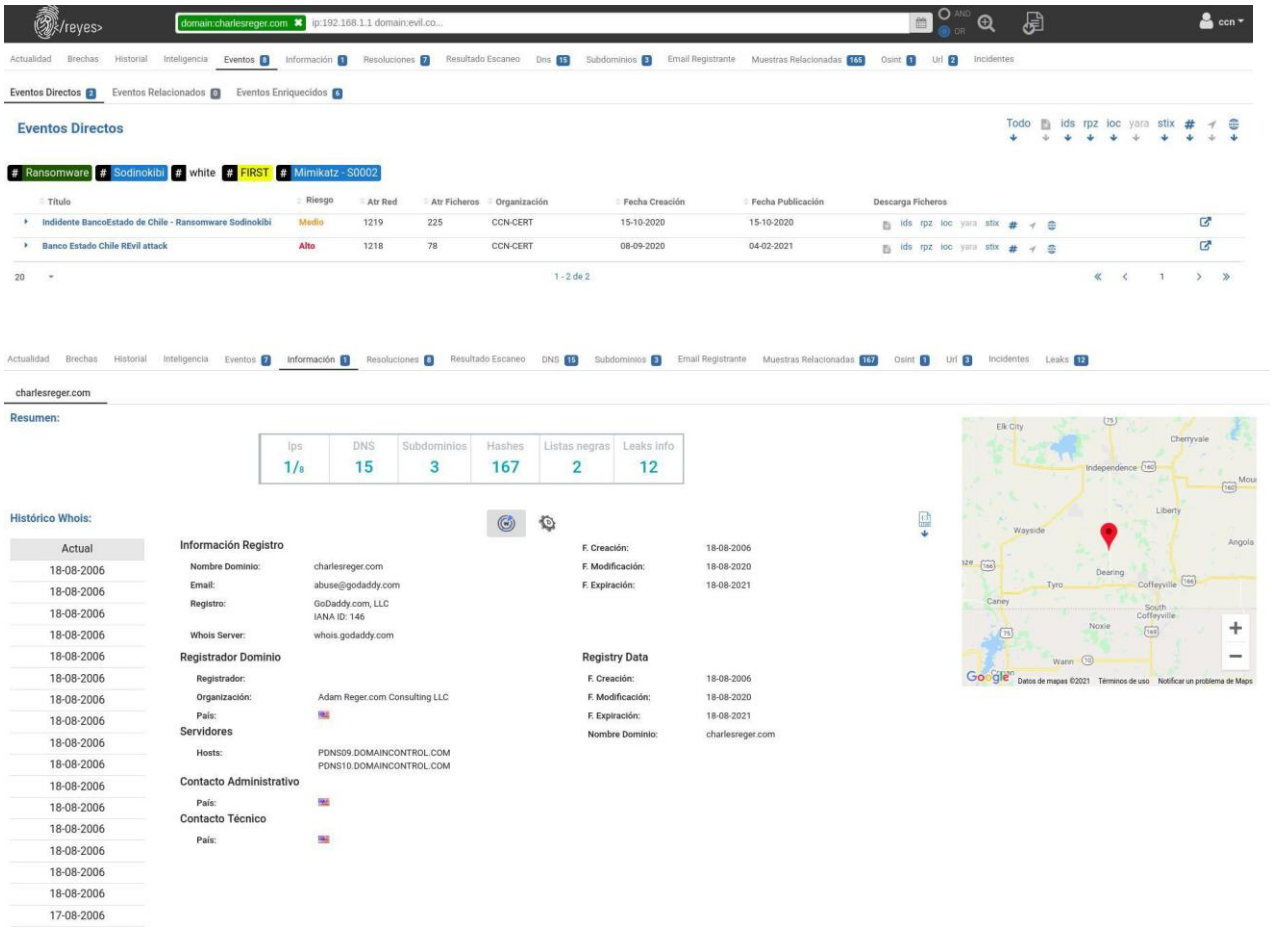




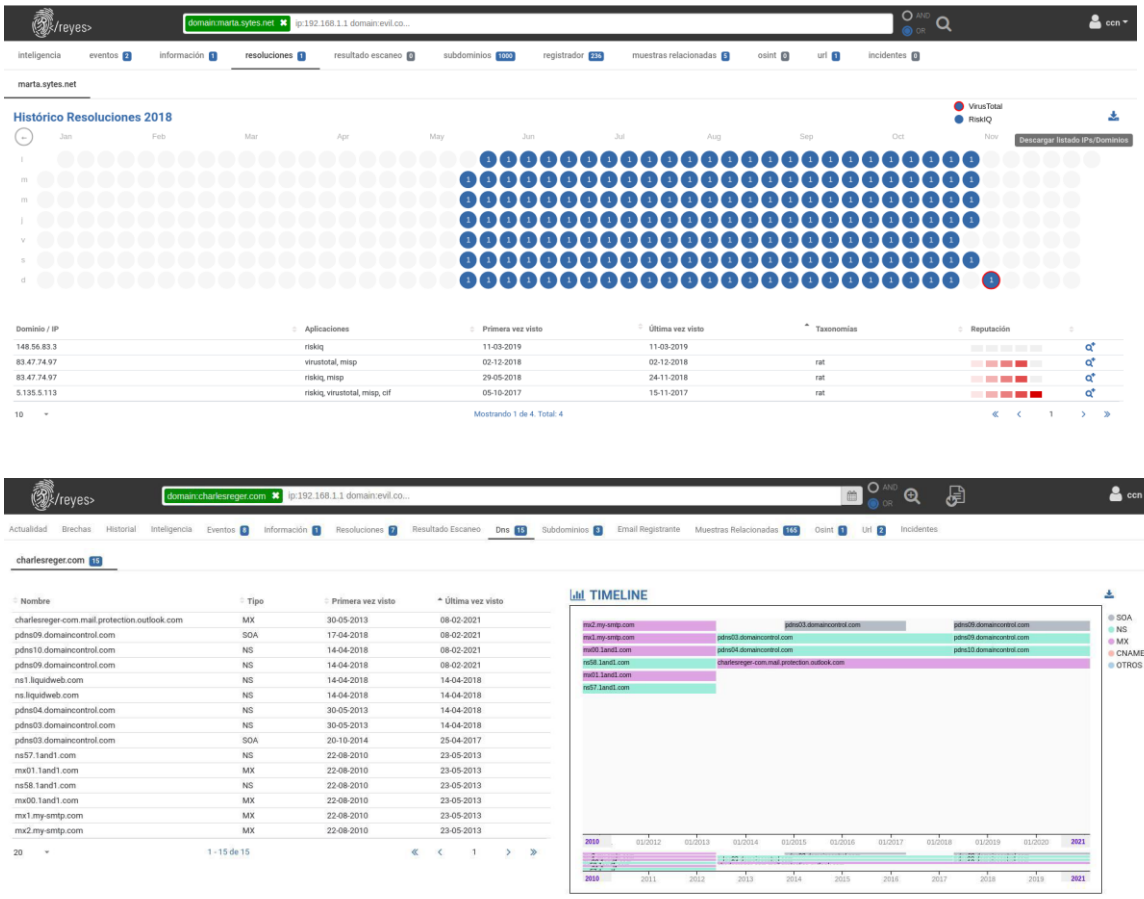
REYES



o

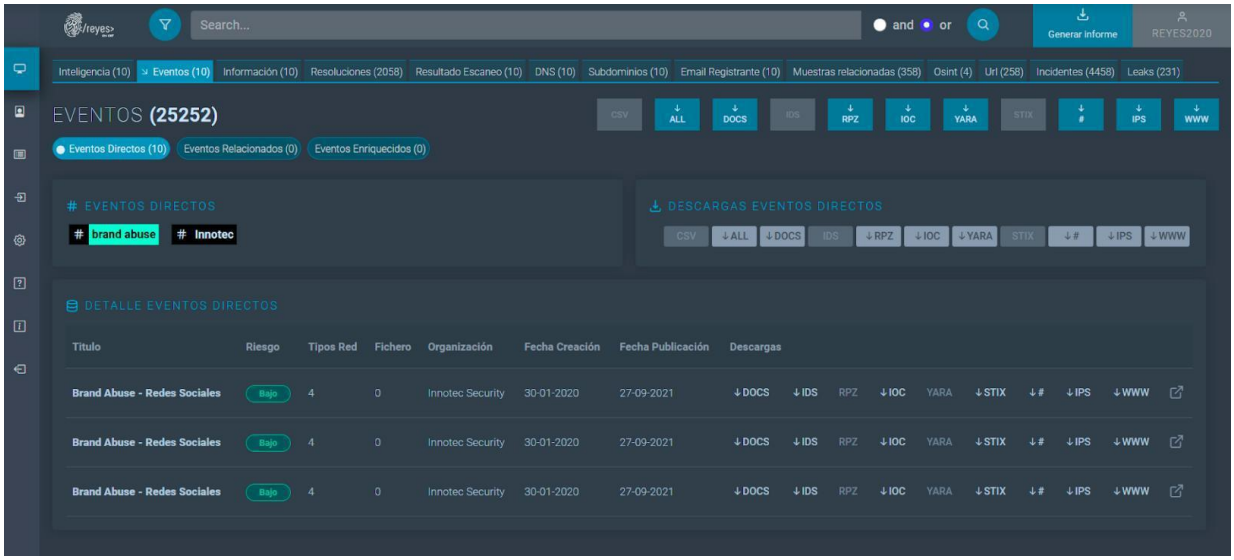


Interfaz REYES



Opciones REYES

Reyes 4.0:



REYES 4.0

Como alternativa open source existe Cortex integrada con la plataforma de gestión de incidentes The Hive, en la que analiza direcciones IP, correos electrónicos, URL´s, nombres de dominio, archivos, hash, todo ello mediante una interfaz web. Los analistas también pueden automatizar estas operaciones y enviar grandes conjuntos de IOC´s desde TheHive o a través de la API REST de Cortex desde plataformas SIRP alternativas, scripts personalizados o MISP. Cuando se usa junto con TheHive, Cortex facilita en gran medida la fase de contención gracias a sus funciones de respuesta activa. Hablando de las herramientas de OSINT se puede usar aparte de shodan, la herramienta open source Spiderfoot, una herramienta de inteligencia automatizada donde proporcionara información relativa a nombres de usuarios, nombres de personas, números de teléfono, correos electrónicos…etc. En respecto a brechas de información se puede usar la herramienta de pago Trillion, para monitorizar cuando se sufra una fuga de datos en la empresa. Se podrán usar más herramientas open source como, por ejemplo:

Análisis de malware: Volatility, FTK, Ghidra e IDA PRO, reglas Yara, para el análisis de malware de memoria para la investigación digital y técnicas forense. Se refiere al acto de analizar una imagen de memoria volcada de una máquina objetivo después de ejecutar el malware para obtener múltiples cantidades de artefactos como por ejemplo información de red, procesos en ejecución, enlaces API, módulos cargados del kernel…etc. Refiriéndose a forense digital el SOC deberá contar con herramientas como CAINE SO, Autopsy, SANS SIFT…etc.

SOAR: Se usarán las herramientas de respuesta automática que integra el SIEM Onion Security, aunque también existen otras como Demisto. Son importantes este tipo de herramientas para automatizar respuestas, así se consigue no fatigar al analista con falsos positivos.

MISP: Malware Information Sharing Platform o simplemente MISP es una plataforma de intercambio de amenazas de código abierto donde los analistas colaboran y comparten información sobre las últimas amenazas entre ellos. Con Reyes y MISP se tienen plataformas de inteligencia e información compartida en tiempo real e integradas.

Herramientas de auditoría: se usará Kali Linux, sistema operativo Linux para realizar actividades de pentesting que integra numerosas herramientas como NMAP, Metaesploit, Nessus, atomic red team para simulaciones automatizadas de ataques…etc.

MITRE: es un sistema de emulación de adversario automatizado que realiza un comportamiento de adversario posterior al compromiso dentro de las redes de. Usa un sistema de planificación y un modelo adversario preconfigurado basado en el proyecto Adversarial Tactics, Techniques &

Common Knowledge (ATT&CK™), así se podrá ver técnicas y tácticas de ataque para poder generar casos de uso, integrarlos en el SIEM y detectarlos.

Wireshark y TCPdump: herramientas para estudiar y analiza el tráfico de red. Se guardará el tráfico de red de día en día para poder analizarlos en manual o con herramientas de inteligencia artificial. Aparte el SIEM trae una herramienta propia para ello.

Threat Hunting: aquí se puede ver la solución del CCN llamada Carmen la cual se monitorizará el proceso número uno de sysmon (system monitor), que se identifica con la creación de nuevos procesos. Aparte el SIEM traerá su herramienta propia para ello.

Honeypot: el propio SIEM integra una herramienta para esta funcionalidad, simulará una máquina la cual generará alertas si es atacada. Se basa en el engaño para atraer a los atacantes y convencerlos de que interactúen. Sin que el atacante lo sepa, recibe una alerta cuando ocurre esa interacción y puede comenzar la investigación del analista.

3.3 Ejemplos de contratos.

Como se ha mencionado anteriormente, aunque se pueden aceptar contratos del sector privado, este trabajo se centrará en el sector público al implementar las herramientas Lucía y Reyes que son las mínimas que hay que tener según el ENS y pasar la certificación.

Para ello, se va a acercarse a la realidad y en la web de contrataciones del estado y se busca por el ámbito de ciberseguridad para encontrar expedientes acordes y que se puedan licitar cumpliendo los requisitos. Estos contratos del Estado van a adjudicarse por puntos valorando muchos criterios como formación al personal de las administraciones, presupuesto, soporte, apoyo con los incidentes…etc.

Expediente: PR-SE-59/2021

ENTIDADES LOCALES>Castilla y León>Valladolid>Ayuntamientos>Valladolid

Órgano de Contratación	Concejalía Delegada de Planificación y Recursos del Ayuntamiento de Valladolid
Estado de la Licitación	Resuelta
Objeto del contrato	Despliegue de un Oficina Técnica de Seguridad y Centro de Operaciones de Ciberseguridad (SOC), diversas soluciones de ciberseguridad y acondicionamiento del CPD de respaldo del Ayuntamiento de Valladolid.
Presupuesto base de licitación sin impuestos	2.424.683,88 Euros
Valor estimado del contrato:	3.186.822,31 Euros
Tipo de Contrato:	Servicios
Código CPV	72000000-Servicios TI: consultoría, desarrollo de software, Internet y apoyo., 30200000-Equipo y material informático., 50300000-Servicios de reparación, mantenimiento y servicios asociados relacionados con ordenadores personales, equipo de oficina, telecomunicaciones y equipo audiovisual., 51610000-Servicios de instalación de ordenadores y de equipo para procesamiento de la información., 72100000-Servicios de consultoría en equipo informático., 72200000-Servicios de programación de «software» y de consultoría., 72500000-Servicios informáticos.
Lugar de Ejecución	España - Valladolid - Valladolid
Procedimiento de contratación	Abierto

Expediente contrato

Memoria justificativa: https://contrataciondelestado.es/wps/wcm/connect/7281b93f-c748-4d01-95ce-b18bf61e16bb/DOC202201141011472021-59_MEMORIA_OT+Ciberseguridad.pdf?MOD=AJPERES

Adjudicación: https://contrataciondelestado.es/wps/wcm/connect/a58885f3-4fe2-4097-b3ce-41dfa0422793/DOC202206090953402021-59_NOTFICACION+GENERICA+PCSP.pdf?MOD=AJPERES

Expediente: 258/2022

ENTIDADES LOCALES>Castilla y León>Salamanca>Ayuntamientos>Salamanca

Órgano de Contratación	Alcaldía del Ayuntamiento de Salamanca
Estado de la Licitación	Resuelta
Objeto del contrato	Suministro, implantación, puesta en marcha y operación de un Centro de Operaciones de Ciberseguridad en el Ayuntamiento de Salamanca, cofinanciado por la Unión Europea - Next Generation EU.
Presupuesto base de licitación sin impuestos	269.269,80 Euros
Valor estimado del contrato:	468.139,80 Euros
Tipo de Contrato:	Servicios
Código CPV	72000000-Servicios TI: consultoría, desarrollo de software, Internet y apoyo., 72200000-Servicios de programación de «software» y de consultoría., 72267000-Servicios de mantenimiento y reparación de software., 72500000-Servicios informáticos.
Lugar de Ejecución	España - Salamanca
Procedimiento de contratación	Abierto

Expediente 258/2022

https://contrataciondelestado.es/wps/wcm/connect/b9a72ec3-bff9-4cf8-ad83-86ed24173e08/DOC20220511110724INICIO.pdf?MOD=AJPERES

Expediente: 79/22 AYTOPARLA

ENTIDADES LOCALES>Comunidad de Madrid>Ayuntamientos>Parla

Órgano de Contratación	Junta de Gobierno del Ayuntamiento de Parla
Estado de la Licitación	Evaluación
Objeto del contrato	Suministro e implementación del centro de operaciones de ciberseguridad y adecuación al esquema nacional de seguridad del Ayuntamiento de Parla
Presupuesto base de licitación sin impuestos	691.105,38 Euros
Valor estimado del contrato:	868.818,19 Euros
Tipo de Contrato:	Suministros
Código CPV	30200000-Equipo y material informático., 48000000-Paquetes de software y sistemas de información., 72000000-Servicios TI: consultoría, desarrollo de software, Internet y apoyo., 79417000-Servicios de consultoría en seguridad.
Lugar de Ejecución	España - Madrid
Procedimiento de contratación	Abierto

Expediente 79/2022

Hay que centrarse en este último y se ven los requisitos que exigen:

-Acreditación de la solvencia económica y financiera:

- Artículo 87 apartado/s:

- Requisitos mínimos de solvencia y acreditación documental: Para garantizar la solvencia económica o financiera los licitadores deberán acreditar mediante declaración responsable, una cifra anual de negocios mínima en los tres últimos años en el ámbito objeto de este procedimiento. La cifra anual de negocios exigida es de 496.000 € referido al mejor ejercicio dentro de los tres últimos disponibles en función de las fechas de constitución o de inicio de actividades del empresario.

Acreditación económica

El equipo de trabajo que llevará a cabo el proyecto estará compuesto al menos por:

- 1 Coordinador del Servicio: Será un consultor con al menos cinco años de experiencia en seguridad y con titulación superior.
- 1 Ingeniero de Seguridad: Tendrá experiencia de dos años al menos en el diseño, despliegue y configuración de todas las herramientas a desplegar y en implantación de SGSI (Sistemas de Gestión de Seguridad de la Información)

  Titulación: Ingeniero Superior en Informática o Ingeniero Superior en Telecomunicaciones o equivalente.
- 1 Analista de Seguridad: Tendrá dos años de experiencia en el despliegue, configuración y operación de las herramientas a desplegar y en implantación de SGSI (Sistemas de Gestión de Seguridad de la Información)

  Titulación: Grado en Informática, Ingeniero Superior en Informática o Ingeniero Superior en Telecomunicaciones o equivalente.
- 1 Consultor de ENS: para llevar a cabo las tareas de adecuación al ENS. Tendrá tres años de experiencia en desarrollo y ejecución de Planes de Adecuación al ENS.

La empresa adjudicataria deberá acreditar que la plataforma donde se alberguen datos on cloud deberá estar situada en territorio de la UE, y que está en funcionamiento y prestando servicio a otros clientes en 2022. Todas las comunicaciones con la empresa serán en idioma español, en 24 x 7, así como toda la documentación intercambiada. Por tanto, en caso de que el CPD donde estén alojados los servidores no esté en España, deberá acreditar su capacidad para comunicar en español en régimen 24x7.

Requisitos de personal

11. Habilitación empresarial.

La empresa deberá poseer las certificaciones que se relacionan a continuación o equivalentes y deberá comprometerse a mantenerlas durante los años de vigencia del contrato.

- Certificación acreditada en Esquema Nacional de Seguridad (ENS) a nivel medio.
- La empresa adjudicataria deberá poseer la certificación del Sistema de Gestión de la Calidad siguiendo la norma de referencia UNE-EN ISO 9001.
- Certificación ISO 20000 para gestión de servicios TI
- Certificación correspondiente en cuanto a los Sistemas de Gestión de Seguridad de la Información conforme a la norma ISO 27001.
- Certificación ISO 14000 del Sistema de Gestión Ambiental

Habilitación empresarial

13. Pólizas de seguros.

Procede: SÍ

El adjudicatario deberá tener suscritos los seguros obligatorios y está obligado a suscribir una póliza de seguros, sin franquicia o asumiéndola expresamente el adjudicatario, que cubra los riesgos que puedan producirse durante la ejecución del contrato, que cubra la responsabilidad por todos los daños que puedan ocurrir, ocasionados por las instalaciones o trabajos que se realicen como consecuencia de la ejecución del contrato.

Momento de entrega de las pólizas: Previa a la adjudicación del contrato.

Seguros

Objetivos:

- Intercambio automático y fluido de ciberincidentes con la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes mediante la implantación y operación de la herramienta de gestión de incidentes LUCIA del CCN-CERT que operará en modo federado con el de la Plataforma Nacional.
- Implantación de las tecnologías necesarias que permitan la vigilancia del perímetro y de la red interna implantando tecnologías incluidas en el Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CCN-STIC 105).
- Revisión del despliegue de la herramienta microClaudia del CCN-CERT ya realizado en el Ayuntamiento de Parla.
- Capacidad de recolección y correlación básica de los registros de trazabilidad (logs) necesarios para la vigilancia.

Además, la solución incluirá el cumplimiento de los siguientes requisitos opcionales:

- Despliegue de tecnologías de detección y respuesta en el punto final (EDR) implantando las tecnologías disponibles en el catálogo CCN-STIC 105 o tecnologías homologadas por el CCN equivalentes
- Intercambio de ciberinteligencia con la Plataforma Nacional de Notificación y Seguimiento de Ciberincidentes mediante la integración de la plataforma desplegada con el sistema REYES del CCN-CERT.
- Formación a los equipos técnicos del Ayuntamiento para la administración y operación de la plataforma desplegada.

La implantación de toda la plataforma se realizará atendiendo al Esquema Nacional de Seguridad, sus instrucciones técnicas de seguridad, las guías de seguridad de las tecnologías de la información y las comunicaciones elaboradas por el Centro Criptológico Nacional, cuya tecnología será la base del Centro de Operaciones de Ciberseguridad que se va a desplegar.

Objetivos

Criterios de adjudicación:

La valoración de las ofertas podrá alcanzar una puntuación máxima de 100 puntos. Los criterios para la adjudicación del contrato son:

- Propuesta técnica: 25 puntos.

    - Ajuste general de la propuesta al objeto general del proyecto: Hasta 20 puntos.
    - Ejecución del proyecto, metodología y planificación general y detallada, y equipos de trabajo: Hasta 5 puntos.

-Criterios valorables en cifras o porcentajes: 75 puntos

- Propuesta económica: 30 puntos

Precio costes del suministro e implementación de la solución: 10 puntos.

Precio costes mantenimiento y soporte durante los tres años restantes de contrato: 20 puntos.

- Tiempo de implementación del proyecto: 10 puntos.

Por cada mes de reducción en el tiempo de implementación del proyecto 2 puntos hasta un máximo de 5 puntos.

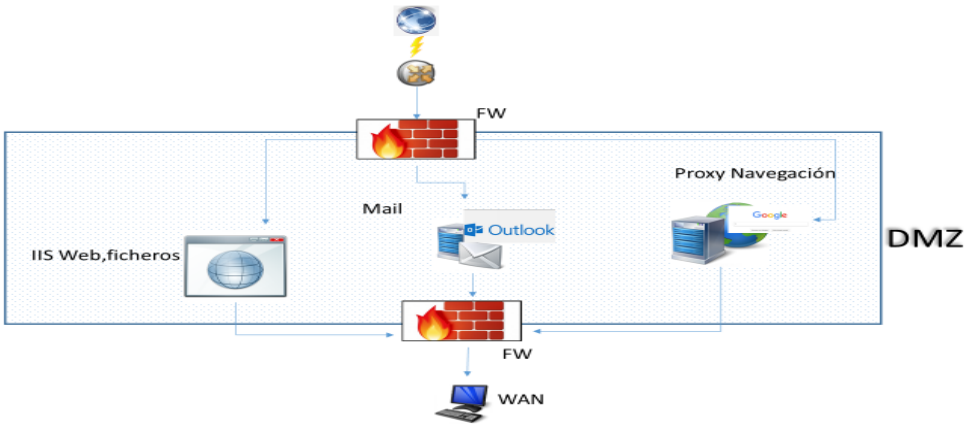
Mejoras propuestas: 35 puntos

- Disponer de un servicio de detección de alertas por personal de la empresa adjudicataria que atienda y gestione las alarmas y alertas generadas fuera del horario laboral, de 15:00h a 8:00h de lunes a viernes y 24 horas fines de semana y festivos: 18 puntos.
- Formación de administradores sobre las herramientas de gestión y sobre la administración de equipos. Por cada jornada adicional sobre las solicitadas 0,5 punto hasta un máximo de 4 puntos.
- Plataforma de formación dedicada para la creación y lanzamiento de contenidos: 2 puntos.
- El sistema de escaneo y gestión de vulnerabilidades en la red incluye un sistema de descubrimiento Shadow IT que permita descubrir cualquier tipo de software o hardware utilizado dentro del Ayuntamiento de Parla sin aprobación ni control del servicio de informática y nuevas tecnologías: 0,5 puntos.
- Capacidad de integración del SIEM con fuentes de inteligencia de amenazas: 1 punto.

- El sistema de recolección, almacenado y gestión de eventos de manera segura tiene capacidad ilimitada de almacenamiento: 1 punto.
- El sistema de recolección, almacenado y gestión de eventos de manera segura tiene capacidad ilimitada de agentes locales a desplegar en sistemas Windows y Linux/Unix: 0,5 puntos.
- Integración de notificaciones del sistema de orquestación y automatización de la seguridad con Telegram: 1 puntos
- Inclusión de pruebas de intrusión (pentesting) adicionales respecto al mínimo indicado de un mínimo de 3 pruebas de intrusión de forma anual: Por cada prueba de intrusión adicional 0,5 puntos hasta un máximo de 1 punto.
- Inclusión de configuraciones de seguridad (hardening) adicionales respecto al mínimo indicado de una vez al año: Por cada configuración de seguridad adicional 0,5 puntos hasta un máximo de 1 punto.
- Inclusión de revisiones de la arquitectura de los sistemas y redes adicionales respecto al mínimo indicado de una revisión anual: Por cada revisión adicional 0,5 puntos hasta un máximo de 1 punto.
- Inclusión de cursos adicionales respecto al mínimo indicado de 4 cursos de 3 horas de forma anual: Por cada curso adicional 0,5 puntos hasta un máximo de 2 puntos.
- Inclusión de campañas de sensibilización adicionales respecto al mínimo indicado de una semestralmente: Por cada campaña adicional 0,5 puntos hasta un máximo de 1 punto.
- Inclusión de campañas de concienciación sobre seguridad en el teletrabajo respecto al mínimo indicado de una semestralmente: Por cada campaña adicional 0,5 puntos hasta un máximo de 1 punto.

3.4 Requerimientos de red y hardware.

Referente a la electrónica de red se considera que está ya implementada ya que en el contrato de licitación no menciona dispositivos para la DMZ. Se considera que se tiene un esquema de red similar a este:



Ejemplo de DMZ

Existen contratos de licitación de suministros de electrónica de red, con lo cual se obvia el implementar lo con el presupuesto. Lo que si se exige es un CPD, aquí se adquieres la solución propia del SIEM que se va a implementar:

	Model	Use Case(s)	Forward Throughput †	Max Storage *	Form Factor
	500	Forward node in a branch office	500 Mbps	8 TB	1U
	1000	Standalone node in a small organization Forward node in a medium office	1 Gbps	24 TB	1U
	1000F	Standalone node in a small organization w/ fiber Forward node in a medium office w/ fiber	1 Gbps	24 TB	1U
	4000	Forward node in a data center Standalone node in a medium to large office	4 Gbps	120 TB	2U

Equipos Security Onion

	10000	Forward node in a large data center (alerts and metadata)	10 Gbps ‡	7 TB	1U
	MN	Manager node in a distributed architecture Manager Search node in a small distributed architecture	N/A	15 TB	1U
	SN7200	Search node in a distributed architecture Manager Search node in a medium distributed architecture Warm Search node in a large distributed architecture Standalone node in a medium to large office	N/A	72 TB	2U
	SNNV	Search node in a distributed architecture Manager Search node in a medium distributed architecture Hot Search node in a large distributed architecture Standalone node in a medium to large office or data center	N/A	30 TB	1U
Response Ready		GoFast	Rapidly deployable incident response High mobility for commercial transportation (all node types supported)	10 Gbps	120 TB	ATA
Response Ready		GoBig	Rapidly deployable incident response High mobility for commercial transportation (all node types supported)	10 Gbps ‡	165 TB	ATA

Hardware Security Onion

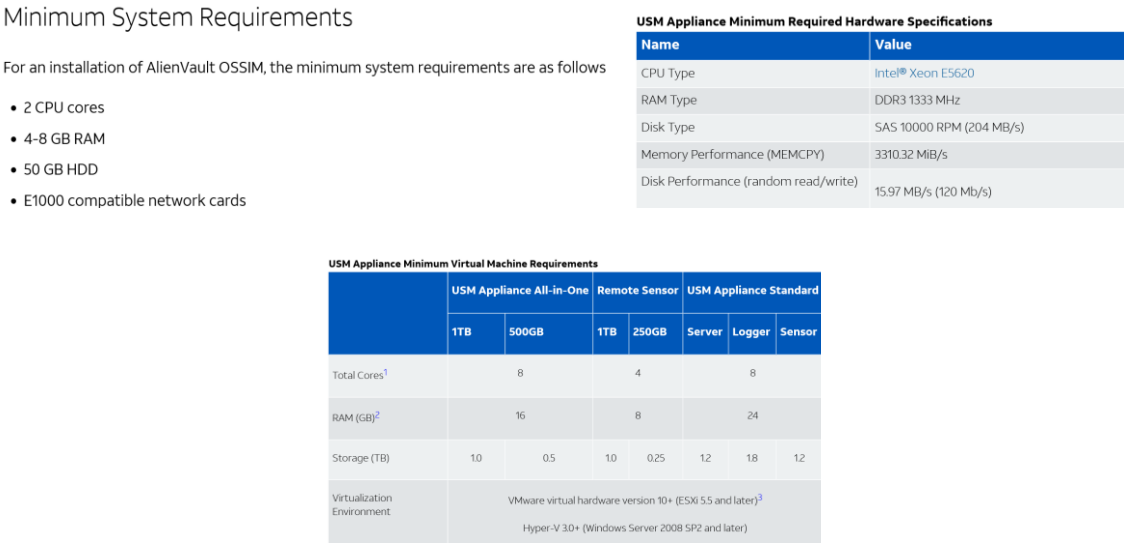
Aquí se tienen todas las opciones posibles. Para elegir la adecuada se estudia la cantidad de máquinas del ayuntamiento. Se ve por información pública que hay 750 funcionarios, con lo cual se supone que se va a monitorizar 750 como mínimo hasta 900 máquinas. Con lo cual se elegiría el modelo 4000. Se muestra el total personal ayuntamiento:

III Personal Funcionario/Laboral		
DENOMINACIÓN	**GRUPO PROF.**	**PLAZAS**
DIRECTOR GENERAL	A1	3
JEFE DE SERVICIO	A1	9
SECRETARIA DE ALCALDIA	C2	1
SECRETARIO/A DE ÁREA	C2	12
Total plazas de Funcionarios/Laborales		**25**
IV Personal Eventual		
DENOMINACIÓN		**PLAZAS**
PERSONAL EVENTUAL		11
SECRETARIO GRUPO POLÍTICO		8
Total plazas de Eventuales		**19**
Total Plantilla Ayuntamiento de Parla		**754**

Personal

https://sede.ayuntamientoparla.es/portal/sede/RecursosWeb/DOCUMENTOS/1/0_6904_1.pdf

Aparte se requiere otro appliance para OSSIM ateniéndose a sus requisitos mínimos como figura el fabricante ya sea físico o virtual:



Minimum System Requirements

For an installation of AlienVault OSSIM, the minimum system requirements are as follows

- 2 CPU cores
- 4-8 GB RAM
- 50 GB HDD
- E1000 compatible network cards

USM Appliance Minimum Required Hardware Specifications

Name	Value
CPU Type	Intel® Xeon E5620
RAM Type	DDR3 1333 MHz
Disk Type	SAS 10000 RPM (204 MB/s)
Memory Performance (MEMCPY)	3310.32 MiB/s
Disk Performance (random read/write)	15.97 MB/s (120 Mb/s)

USM Appliance Minimum Virtual Machine Requirements

	USM Appliance All-in-One		Remote Sensor		USM Appliance Standard		
	1TB	500GB	1TB	250GB	Server	Logger	Sensor
Total Cores[1]	8		4		8		
RAM (GB)[2]	16		8		24		
Storage (TB)	1.0	0.5	1.0	0.25	1.2	1.8	1.2
Virtualization Environment	VMware virtual hardware version 10+ (ESXi 5.5 and later)[3] Hyper-V 3.0+ (Windows Server 2008 SP2 and later)						

Requisitos SIEM

Se tendrá otro appliance opcionalmente para CARMEN como herramienta de threat hunting, estos son los requisitos:

"CARMEN se distribuye en un appliance físico con las siguientes características: 2 CPU de 8 núcleos cada uno, 64 GB RAM, 2 HDD en RAID10 de 300GB cada uno y 2 HDD de 600GB para el almacenamiento. Tiene además una fuente de alimentación redundante y 8 interfaces de red en dos tarjetas de cuatro interfaces cada una."

Aparte se tendrá otro appliance de requerimientos estándar para aplicaciones propias de terceros que ayuden en el día a día.

3.5 Propuesta económica.

A continuación, se va a evaluar los ingresos y los gastos. Se presenta ingresos del contrato:

Anualidad	Importe (con IVA)
2022	477.850,01 €
2023	119.462,50 €
2024	119.462,50 €
2025	119.462,50 €

El presupuesto máximo de licitación para será de 691.105,38 € más IVA para los cuatro años de contrato. El precio se debe desglosar en los siguientes apartados:

Presupuesto

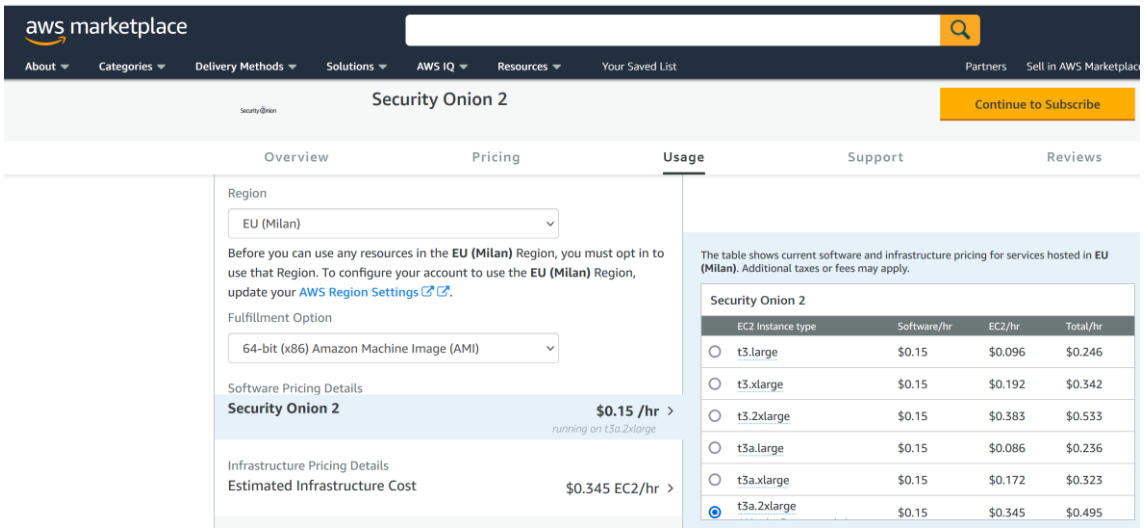
Como gastos se tienen:

- Personal que como mínimo será de: coordinador del servicio, ingeniero de seguridad, analista de seguridad y un consultor del ENS. El personal se encarga de la implantación, mantenimiento, charlas de formación, plataforma de formación propia o subcontratada y gestionar las alarmas y alertas generadas fuera del horario laboral, de 15:00h a 8:00h de lunes a viernes y 24 horas fines de semana y festivos.
- Soluciones CCN obligatorias Lucía y opcionales Reyes, MISP y CARMEN.
- Póliza de seguros obligatoria.
- Formación del personal ya sea cursos, certificaciones…etc.
- Gastos en certificaciones: ENS, ISO 9001/20000/27001/14000.
- CPD: Para el cálculo de los 3 appliance se va a ir uno por uno y se valoran precios de computación en la nube.
- Dos appliance (1 de back-up) para Carmen(opcional), Lucía, OSSIM y resto de aplicaciones. 10.000€ aproximado.
- Dos Appliance SIEM Onion Security: ¿modelo 4000€, precio no facilitado por la empresa para fines domésticos…20.000€?
- EDR (opcional) 7 euros al mes/host, unos 5.000€/mes.

Ahora se analizan precios de computación en la nube si no se quiere invertir en hardware con el SIEM principal. Se recuerda que el requisito era el siguiente:

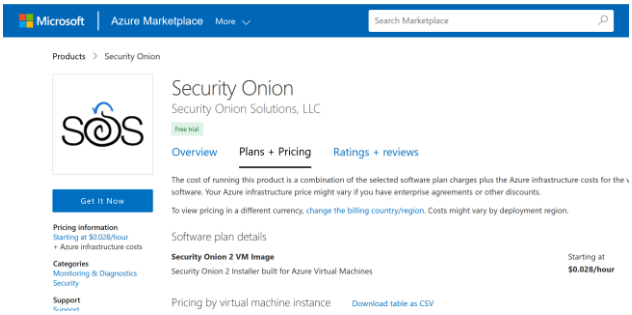
"La plataforma donde se alberguen datos on cloud deberá estar situada en territorio de la UE, y que está en funcionamiento y prestando servicio a otros clientes en 2022. Todas las comunicaciones con la empresa serán en idioma español, en 24 x 7, así como toda la documentación intercambiada. Por tanto, en caso de que el CPD donde estén alojados los servidores no esté en España, deberá acreditar su capacidad para comunicar en español en régimen 24x7."

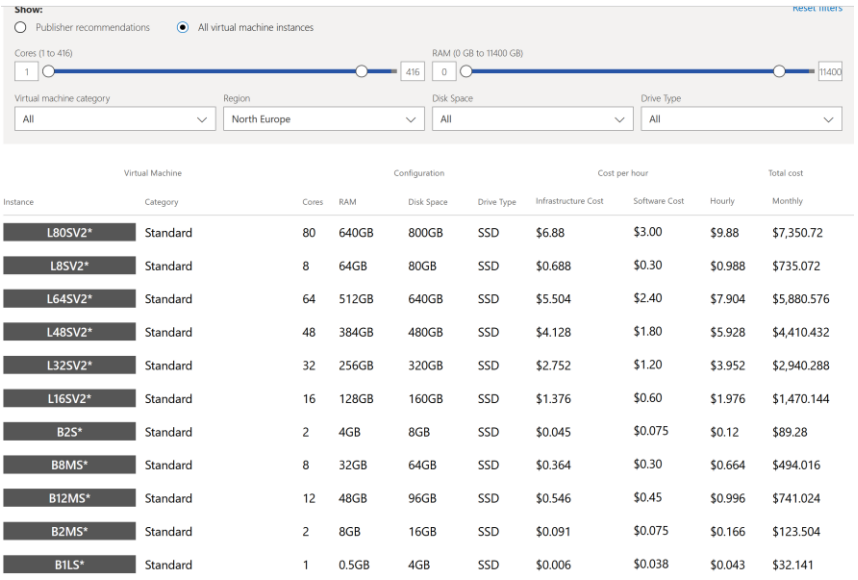
Se comparan precios en servicio de AWS de Amazon:



Precios AWS

Se podrá seleccionar la potencia adecuada incrementando el precio para los appliance que se vaya a montar y poder estudiar su precio. Así mismo para la solución de Microsoft:





Show: Reset filters

Publisher recommendations | All virtual machine instances

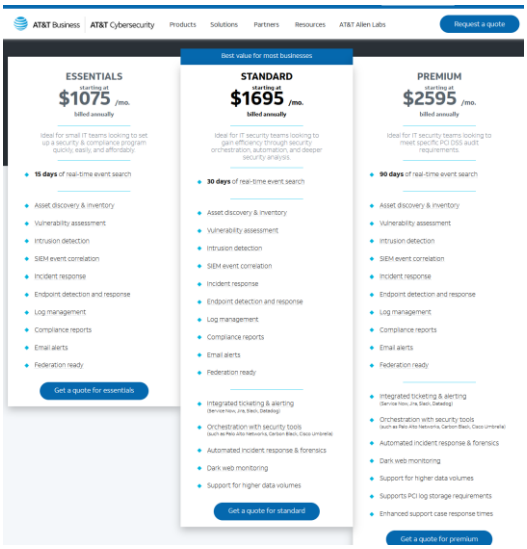
Cores (1 to 416): 1 – 416 | RAM (0 GB to 11400 GB): 0 – 11400

Virtual machine category: All | Region: North Europe | Disk Space: All | Drive Type: All

Virtual Machine		Configuration				Cost per hour			Total cost
Instance	Category	Cores	RAM	Disk Space	Drive Type	Infrastructure Cost	Software Cost	Hourly	Monthly
L80SV2*	Standard	80	640GB	800GB	SSD	$6.88	$3.00	$9.88	$7,350.72
L8SV2*	Standard	8	64GB	80GB	SSD	$0.688	$0.30	$0.988	$735.072
L64SV2*	Standard	64	512GB	640GB	SSD	$5.504	$2.40	$7.904	$5,880.576
L48SV2*	Standard	48	384GB	480GB	SSD	$4.128	$1.80	$5.928	$4,410.432
L32SV2*	Standard	32	256GB	320GB	SSD	$2.752	$1.20	$3.952	$2,940.288
L16SV2*	Standard	16	128GB	160GB	SSD	$1.376	$0.60	$1.976	$1,470.144
B2S*	Standard	2	4GB	8GB	SSD	$0.045	$0.075	$0.12	$89.28
B8MS*	Standard	8	32GB	64GB	SSD	$0.364	$0.30	$0.664	$494.016
B12MS*	Standard	12	48GB	96GB	SSD	$0.546	$0.45	$0.996	$741.024
B2MS*	Standard	2	8GB	16GB	SSD	$0.091	$0.075	$0.166	$123.504
B1LS*	Standard	1	0.5GB	4GB	SSD	$0.006	$0.038	$0.043	$32.141

Precios Azure

Precios de USM si se quiere ampliar desde OSSIM.



Precios USM

Costos de personal: uno o dos analistas con un salario de 40.000€ anuales.

3.6. Necesidad de personal.

Si se analiza el contrato de licitación el personal mínimo es cuatro lo cual puede ser un grupo fijo. El único inconveniente que se ve es que de los 35 puntos de baremos 18 son asignados si se ofrece una respuesta a incidentes fuera de horario laboral, de 15:00 a 08:00, festivos y fines de semana, lo cual implica a la semana unas 123 horas semanales más festivos. Si no se presta este servicio con personal cualificado se pierden 18 puntos lo cual son imprescindibles para hacerse con un contrato.

Esto quiere decir que hay que contratar personal para para cubrir parte de esas horas. La idea poco a poco es conseguir más contratos e ir aumentando el personal.

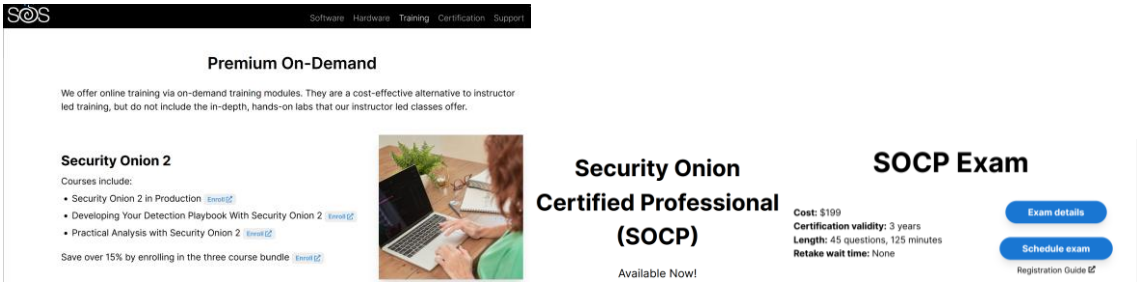
El régimen de contrato ideal sería como se ven en muchas ofertas del extranjero en cuenta propia y en remoto. En cuenta propia para ahorrarse costos en seguridad social y en remoto para que no sea necesario el tener una oficina.

3.7 Cursos de formación.

Hoy en día es casi obligatorio disponer de una formación continua para ser un buen analista de seguridad. La formación para el personal a contratar será como mínimo de analista de nivel 2. Se ofrecerá formación a cargo de la empresa y algún tipo de certificación como, por ejemplo:

Certificaciones

Para el SIEM Onion Security se dispone de formación de pago on-demand y certificación:



Certificaciones Security Onion

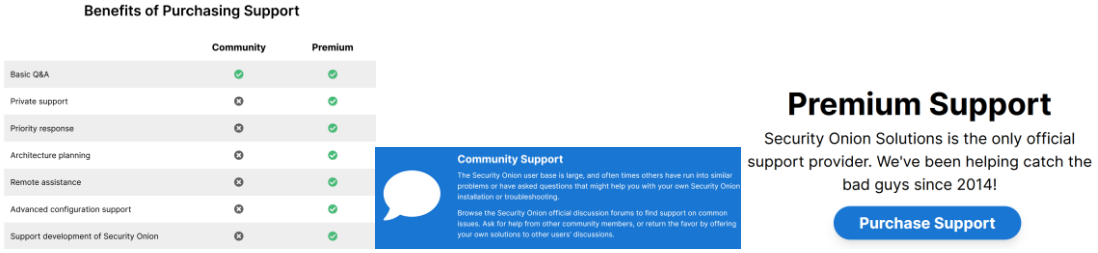
Para personal del ayuntamiento se ofrecerá cursos de formación a través de plataformas comerciales como Udemy, Coursera, Cybrary…etc.

3.8 Servicios de soporte.

Sobre servicio de soporte de las aplicaciones open source normalmente, al ser gratuitas se obtendrá de internet, foros…etc. Es la única desventaja de no ser herramientas comerciales de pago, no se contará con un soporte personalizado. Sin embargo, opcionalmente si se elige Carmen para combatir las APT se tendrá soporte de la empresa que la ha desarrollado y da soporte que es S2 Grupo.

Para el SIEM OSSIM en la web de AT&T se tendrá disponible la comunidad. Para la versión de pago USM habrá un canal de soporte más personalizado ante los problemas que se registren.

En el SIEM Onion Security se dispone de una zona comunitaria de soporte y se dispone de una premium, bastará con una subscripción para elevar la membresía.



Soporte

3.9 Organización del capítulo.

En este capítulo se ha empezado definiendo el tipo de empresa o startup del tipo sociedad limitada acogiéndose a la nueva ley y comparando las ventajas que se tendrán como ayudas, deducciones fiscales y demás.

A continuación, se ha detallado el software elegido, haciendo más hincapié en las herramientas del CCN ya que dos son obligatorias (Lucía y Reyes) para operar en las administraciones públicas. Aparte se ha definido el SIEM principal y secundario, OSSIM y Security Onion.

Se muestran ejemplos de contratos de licitación del estado para ver cómo son y ver que requisitos solicitan, baremo de puntuación y proposiciones económicas. Se cogerá uno de ejemplo y hay que centrarse en él.

Se analizan los requerimientos de red y de hardware. En principio se cuenta con una DMZ y se pondrá el hardware ya sea físico o computación en la nube.

Se pasa a los aspectos económicos siendo algo orientativo beneficios y gastos en general.

Se finaliza hablando de la necesidad de personal a contratar, la formación a impartir al personal y los servicios de soporte que las herramientas tienen.

4. Resultados.

Una vez definidas las herramientas definidas hay que centrarse en la instalación y pruebas en este capítulo. Hay numerosas herramientas, lo cual se hace inviable para el proyecto la instalación y prueba de todas. Obviaré herramientas útiles y fundamentales del SOC.

Como el objetivo es intentar conseguir un contrato de licitación el trabajo se va a centrar en implantar y testear de forma sencilla las siguientes soluciones:

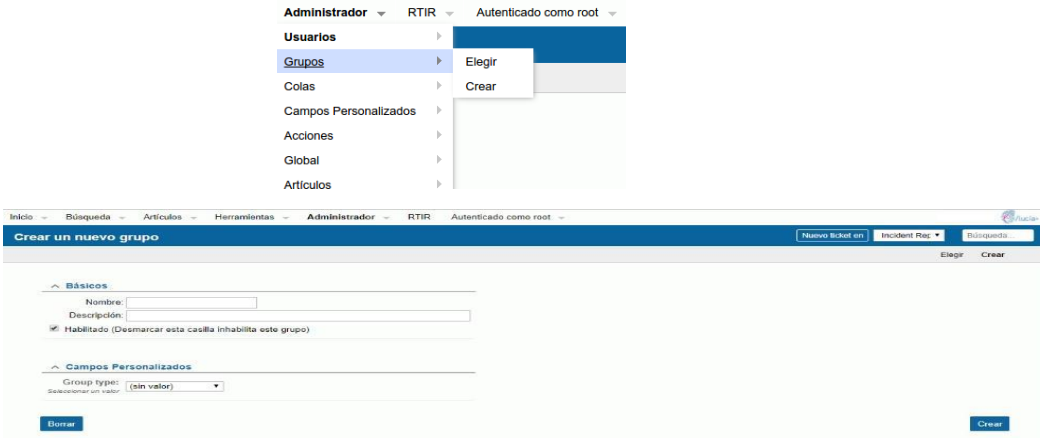
- Gestión de incidentes LUCIA.
- SIEM AlienVault.
- SIEM Security Onion.

4.1 Gestión de Incidentes LUCIA.

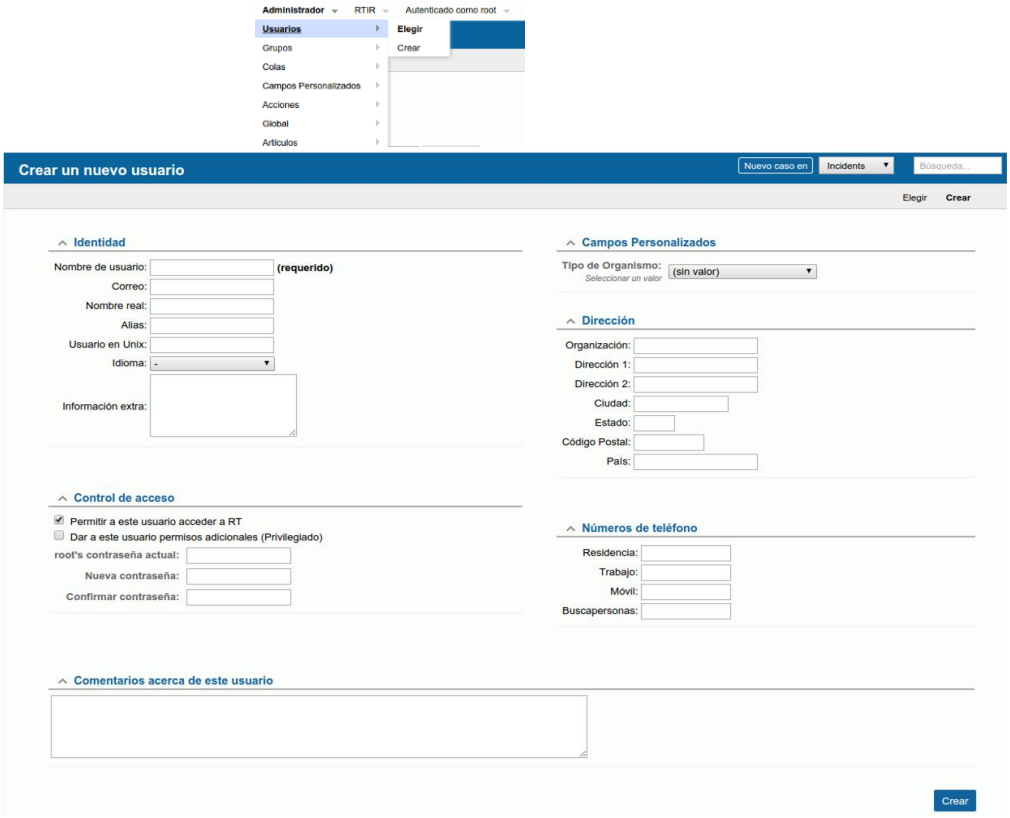
Para la instalación de LUCÍA se seguirá con la guía CCN-STIC 845C en una máquina virtual y para la administración y configuración se plasmará la misma información de las guías CCN-STIC 845A y CCN-STIC 845D.

Una vez instalado se accede a la interfaz web de Lucía. Se puede generar una CA propia, autoridad certificadora y emitir propios certificados auto firmados. Una vez realizado, en la configuración inicial se establecerá el nombre de la máquina, se configurarán fecha y hora.

Se tendrá que configurar el servicio de gestión de tickets editando varios parámetros. Seguidamente se configurará el correo electrónico, se comprobará la comunicación con Lucía central y la sincronización de incidentes. Ahora se explicará la gestión y creación de grupos con usuario root:

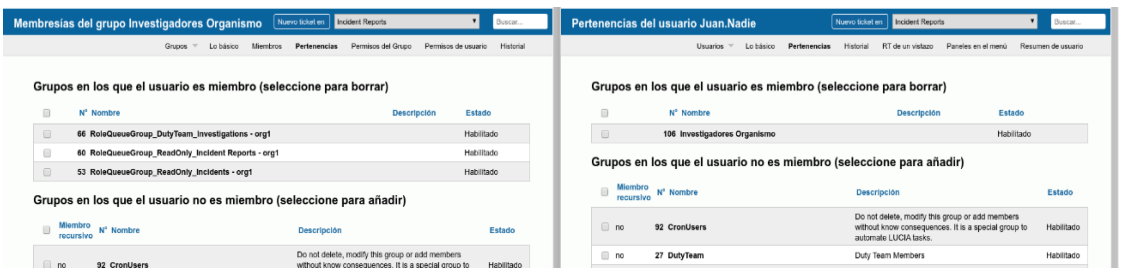


Los atributos del grupo y la metainformación serán asignados. Los grupos son organizados por taxonomía y por rol. Los grupos de rol tienen el formato RoleGroup_<NombreDeRol>, y estos tienen los permisos sobre los campos necesarios para poder usar LUCIA. La gestión de usuarios se tiene que realizar con usuario root. Ejemplo de creación de nuevo usuario:

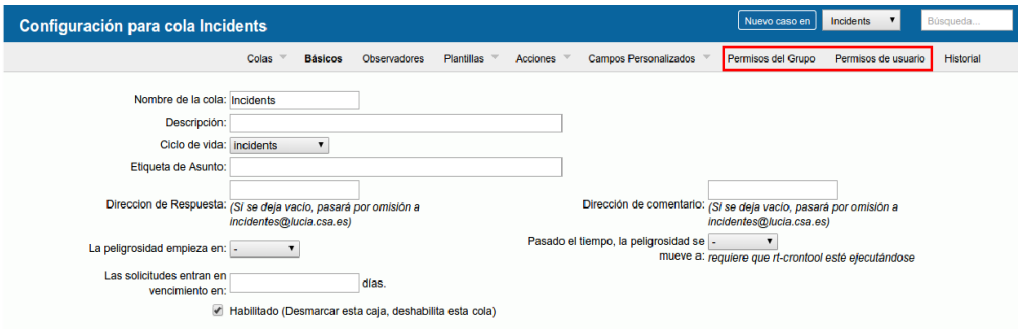


Hay que incluir los atributos y la metainformación de los usuarios. De manera automática al instalar LUCIA se originan los dos usuarios **rest** y **rtcronuser** los cuales no se pueden modificar para que la herramienta funcione sin problemas.

En el siguiente ejemplo, se ve que se añade un usuario a un grupo con permisos para que este pueda crear y modificar investigaciones, pero solo consultar reportes e incidentes:

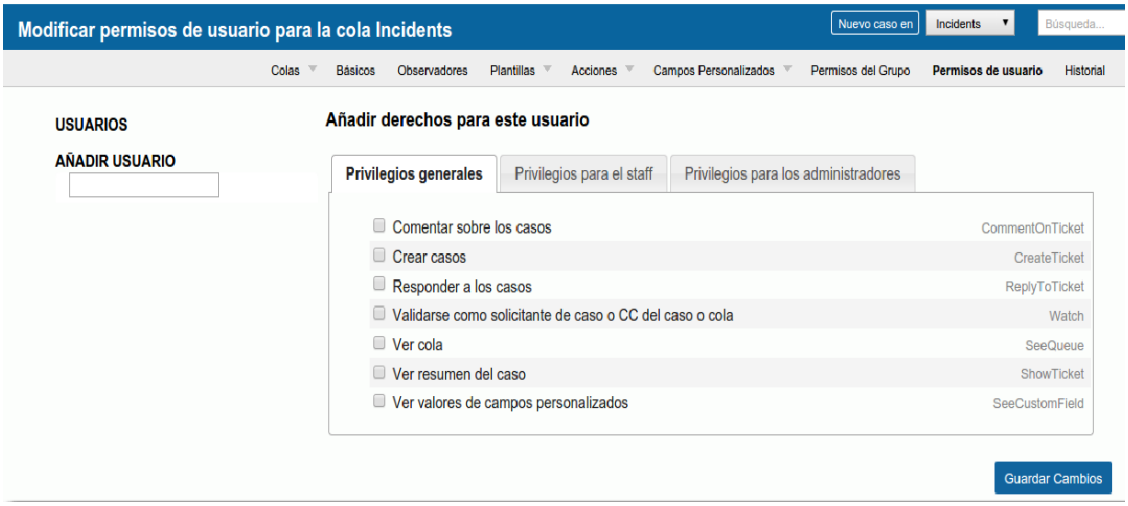


Ahora se vas a ver el concepto de las colas, que es la ordenación de tickets, permisos...etc. Cada cola tiene unos atributos y una metainformación. En cada cola es muy importante que se especifiquen los permisos de usuarios y grupos:

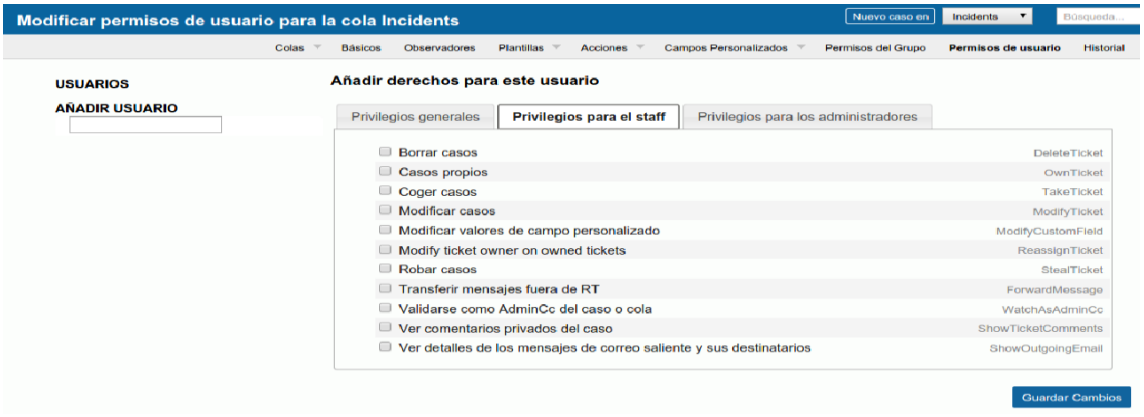


Se tendrá que elegir diferentes tipos de permisos para usuarios y grupos como:

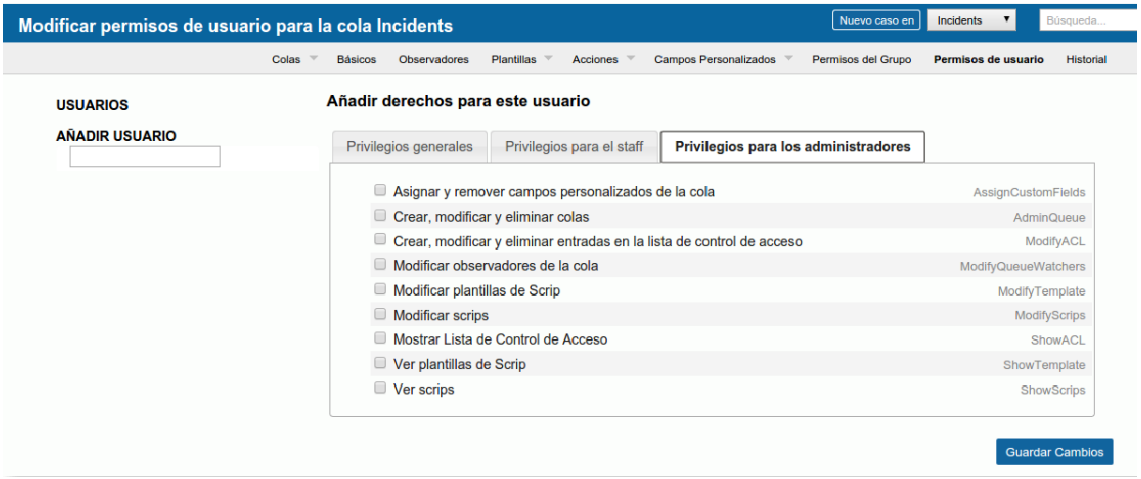
- Permisos generales: Pueden ejecutar acciones básicas sobre la cola y los tickets, como crear un caso, realizar un comentario, responder un caso…



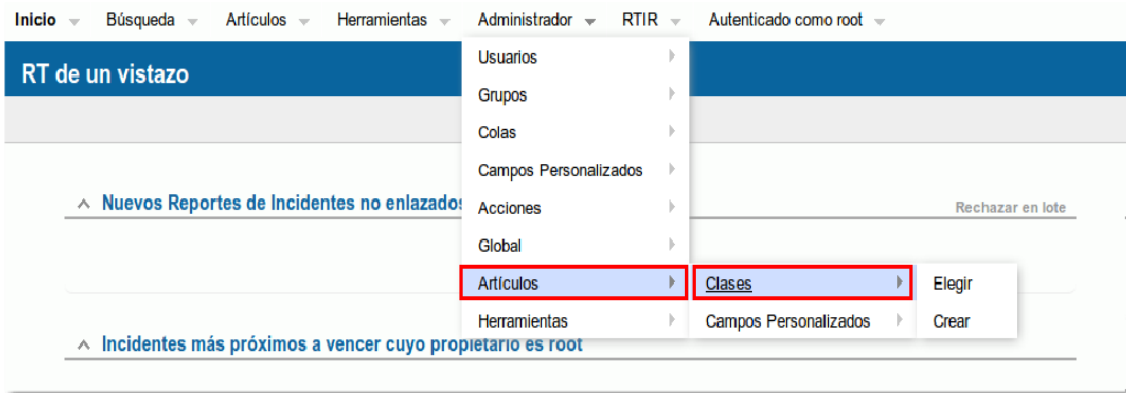
- Permisos para el personal: Son los permisos para realizar gestiones sobre los tickets, como, por ejemplo, el poder modificar campos personalizados, o modificar el ticket, poseer un ticket…etc. Ejemplo de modificación de permisos de usuario en una cola:



- Permisos de administrador: Son permisos para de administrar la cola o un campo personalizado. Se pueden asignar nuevos campos personalizados, como crear/modificar/borrar la cola…etc.



Los artículos realizan respuestas tipo a preguntas muy frecuentes. Se almacena un texto predefinido para usarse de respuesta. La gestión de las clases que equivalen a las colas.
En esa clase los artículos deberían aparecer en un desplegable:



LUCIA es un software de ticketing, para el seguimiento, notificación y trazabilidad de los tickets. LUCIA permite crear una incidencia o ticket y como consecuencia de ello, realizar la investigación correspondiente. A través de LUCIA, se solicita información al usuario que informó de la incidencia, añadir información o empezar una investigación para intentar resolverla.

Las instancias federadas son aquellas instancias propias del organismo que sincronizan los incidentes de una o más colas a través de la red central de sincronización de LUCIA. Una instancia no federada es aquella que está desplegada localmente en el organismo y desconectada de la red de sincronización de LUCIA.

Tickets son la unidad más básica de información de LUCIA. Un ticket está formado por atributos que le suministran información y por más atributos que son su metainformación.

Se podrá afirmar que la cola es la unidad organizativa de tickets. Es una jerarquía lógica donde se organizan los tickets. En las colas se definen los atributos de información de los tickets que se alojaran en ellas.

Se podrá analizar cuatro tipos de tickets: incidentes (propios), incidentes SAT, reportes de incidentes, e investigaciones. Los incidentes SAT corresponden a la sonda SATINET si se tiene contratada.

Reporte de incidente (incident report).
Los correos recibidos en el buzón de entrada monitorizado por LUCIA generan automáticamente un reporte de incidente (IR).

Un reporte de incidente puede o no ser un incidente. En el caso de que sea un incidente, el reporte podrá tener un link al incidente. Un mismo reporte de incidente puede pertenecer a varios incidentes y un mismo incidente puede asociarse a varios reportes de incidentes. Con el reporte de incidente establecemo una vía de comunicación con la persona que notificó la incidencia.

Investigación (investigation).
Con una investigación se inicia una comunicación con usuarios externos e a los reportes de incidentes.

Que una investigación se resuelva no quiere decir que el incidente esté finalizado, por lo que es posible que existan varias investigaciones del mismo incidente. Por el contratio, una investigación sólo puede estar asociada a un incidente.

Incidente (incident).
Es el propio ticket que representa el incidente en sí y puede tener asociados reportes de incidentes e investigaciones.

Al resolver un incidente se cierran todos los reportes de incidentes e investigaciones asociadas dándose por finalizada la gestión del ticket. El incidente es susceptible de sincronización con LUCIA Central.

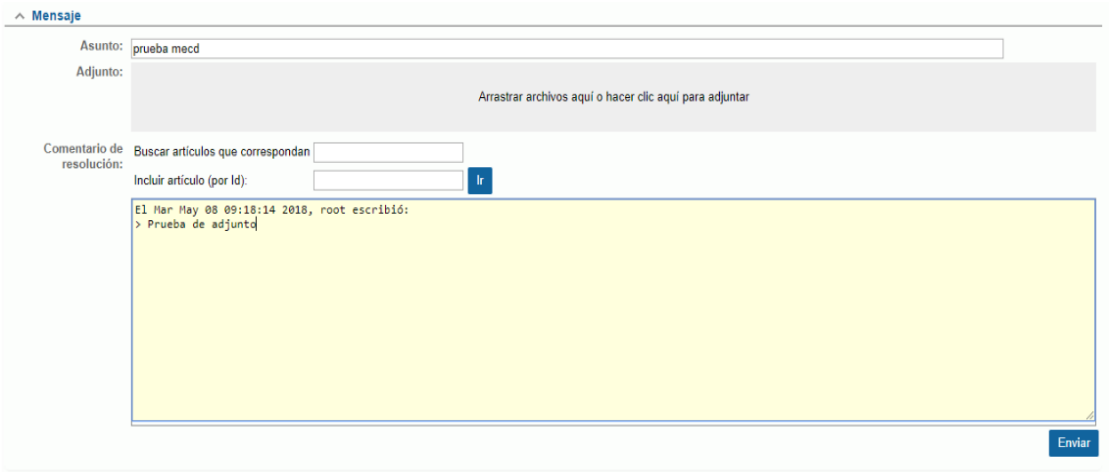
Ciclo de vida de un ticket.

Los estados de un ticket son los siguientes:

- Nuevo (new): Estado por defecto cuando se recibe correo y se genera un reporte de incidente.
- Abierto (open): Estado por defecto cuando se crea un ticket.
- Resuelto (resolved): Indica que el ticket se ha resuelto. Hay que rellenar un campo de resolución para cumplir con el ENS.
- Rechazado/Abandonado (rejected/abandoned).

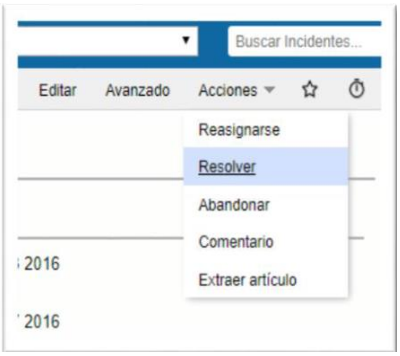
Comentar un incidente.

La actuación de comentar es parecida al de 'Responder', se diferencian de que no existen destinatarios a los que enviar la respuesta, solo se quedará registrada en el incidente.



Resolver (cerrar) un incidente.

Para resolver un incidente, se usará el botón de 'Resolver' bajo el menú 'Acciones'.



En este proceso hay que rellenar todos los campos de resolución de un incidente para cumplimentar los requerimientos del ENS y quedar registrada la información para completar con los requerimientos de INES. Los campos son los siguientes:

– Peligrosidad.

– Resolución.

– Recursos Invertidos.

– Categoría del sistema según ENS.

– Impacto.

– Número de sistemas afectados.

– Causa del incidente.

– Incidencias durante la resolución.

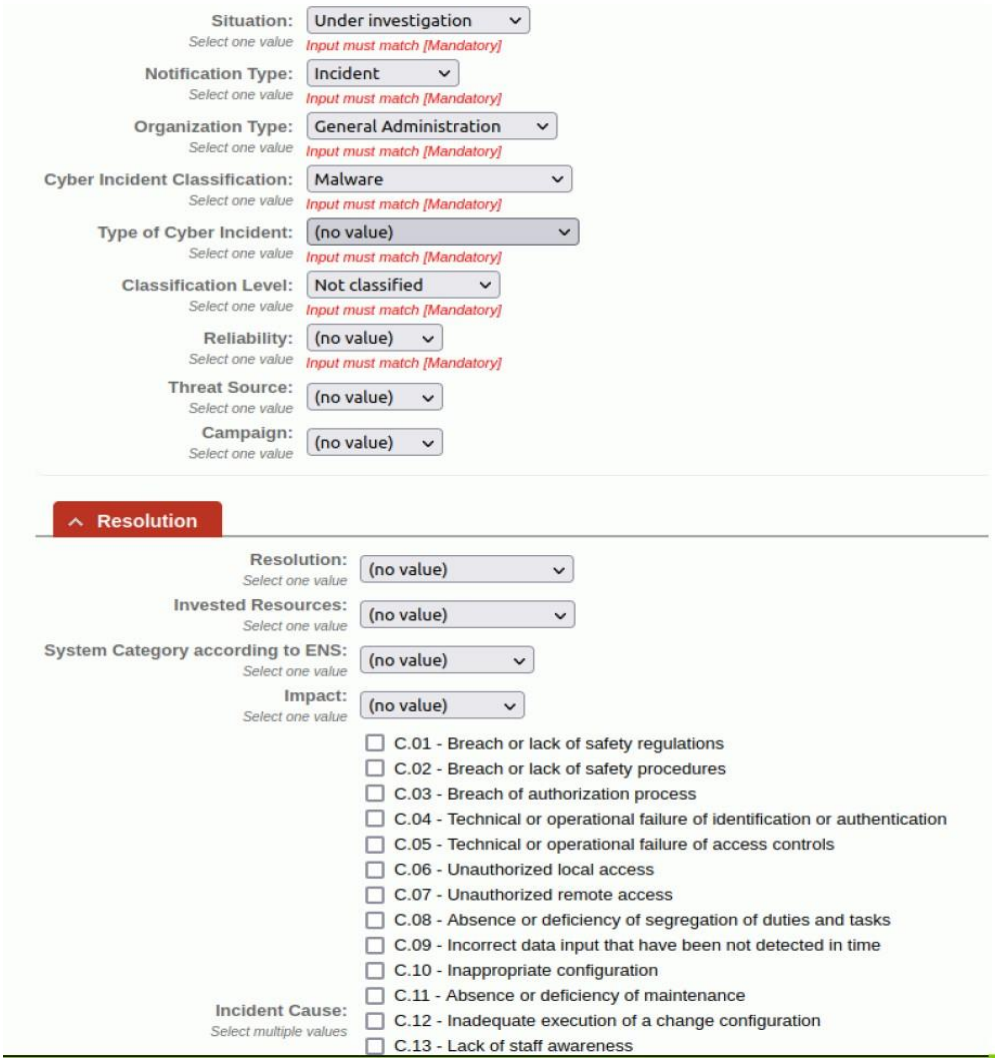
– Tiempo trabajado.

– ¿Afecta al RGPD?

– Notificar a AGPD.

– Notificar al CNPIC.

– Categoría del Sistema según ENS.



Ejemplo de flujo de trabajo.

Un usuario envía un correo a la cuenta de LUCIA notificando que ha sido infectado por malware.

Este correo genera un ticket de reporte de incidente que el operador se asignará para ser su propietario. En caso de que no sea válido o ser un falso positivo el reporte de incidente puede ser rechazado.

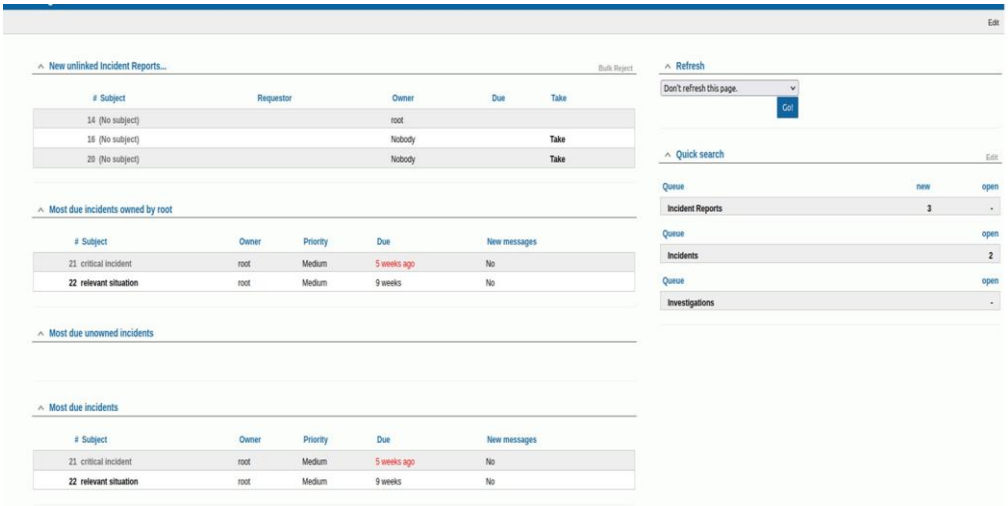
El operador se puede comunicar con este usuario a través del reporte de incidente. Al mismo tiempo, el operador creará un ticket incidente donde volcará la información. Si ya existe un ticket similar al incidente puede ser enlazado.

Si necesita comunicarse con el administrador para solucionar el incidente, realizará una investigación enlazada al incidente para comunicarse con el administrador. El operador puede resolver los reportes de incidentes e investigaciones según se vayan solucionando. Sin embargo, si resuelve el incidente directamente, todos los objetos enlazados se resuelven automáticamente.

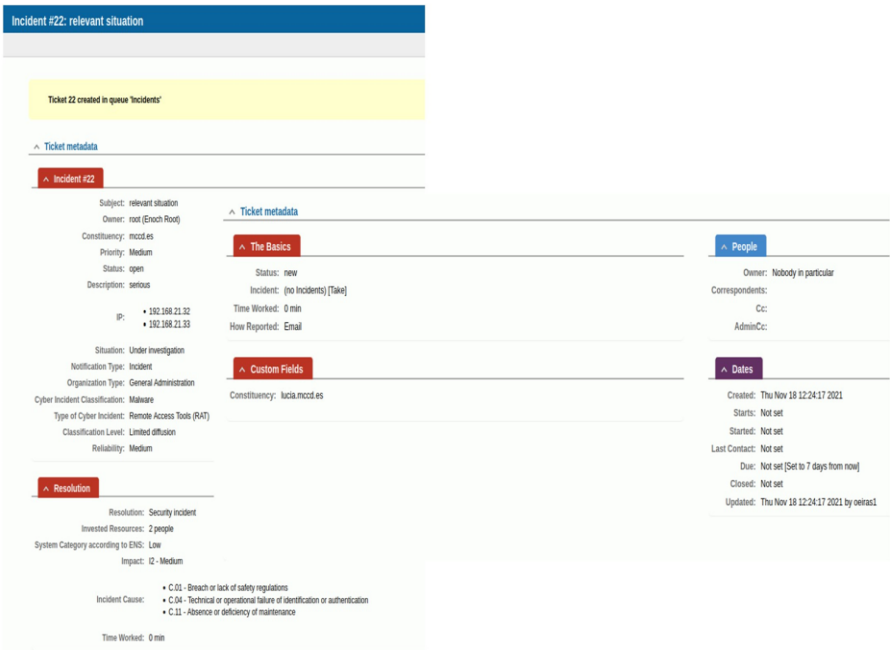
Descripción del panel RTIR.

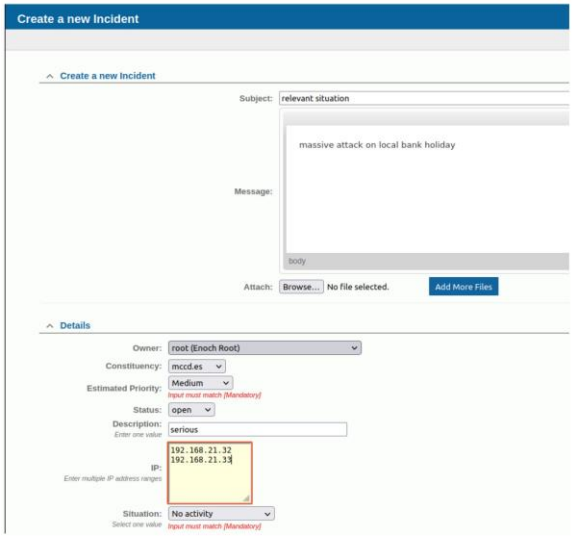
Se recomienda utilizar la vista 'RTIR'. Se pueden ver dos campos: El cuerpo (panel principal) y la barra lateral. Ambos se pueden personalizar:

- Nuevos reportes de incidentes no enlazados.
- Incidentes con fecha tope más cercana sin propietario.
- Incidentes con fecha tope más cercana.



Si se quiere crear un nuevo ticket, se seccionará la cola donde se alojará el ticket:





Asignarse y reasignarse un ticket.

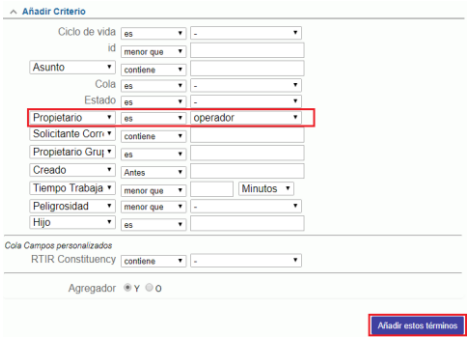
'Asignarse' un ticket es lo primero que hay que hacer para trabajar con él. Es lo mismo que adquirirlo como propietario del mismo. Se tiene que entrar en la vista de un ticket y seleccionar *'Asignarse':*

'Reasignarse' un ticket tiene el mismo significado para que orto operador pueda trabajar sobre él.

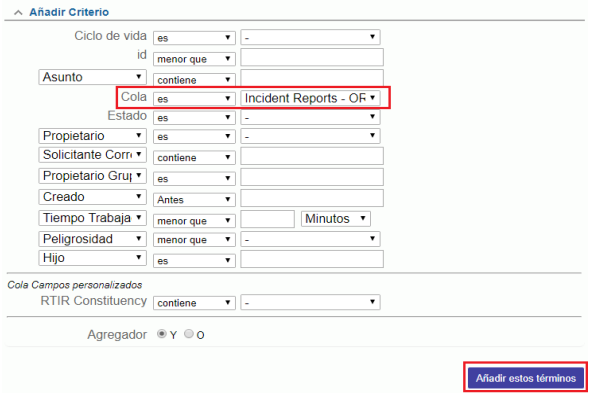
Búsquedas.

Con la opción 'Búsqueda' es posible realizar búsquedas con una lógica similar al lenguaje SQL para encontrar tickets.

Dentro de la página de 'RTIR/Búsqueda/Nueva búsqueda', seleccionar el criterio 'Propietario' 'es' 'nombre_usuario' y pulsar en el botón 'Añadir estos términos'.

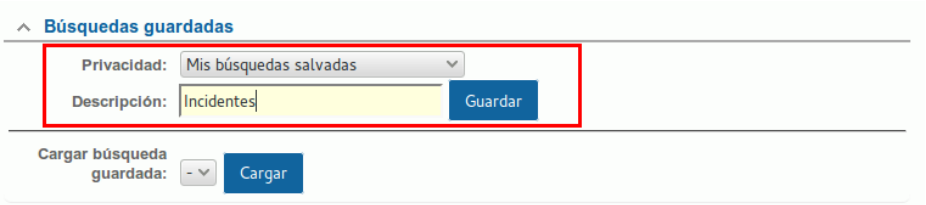


Se selecciona la cola deseada donde se va a buscar, una o varias colas:

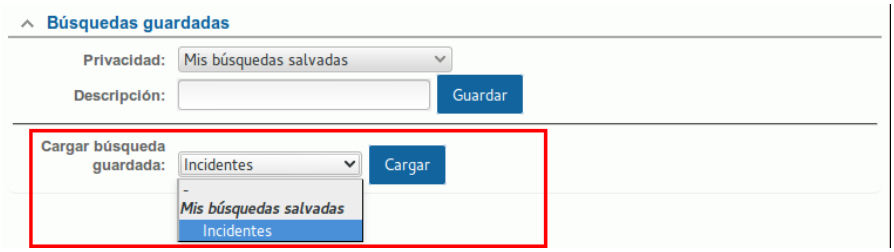


Resultando la siguiente consulta:

Se podrá personalizar las búsquedas, seleccionando todos los campos lo que se esté buscando. Se pueden guardarlas e incluir una descripción.

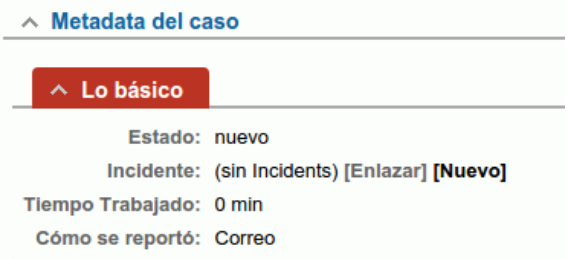


Si se necesita cargar una búsqueda se selecciona en el desplegable 'Cargar búsqueda guardada' y pulsar en el botón "Cargar".



Enlazar.

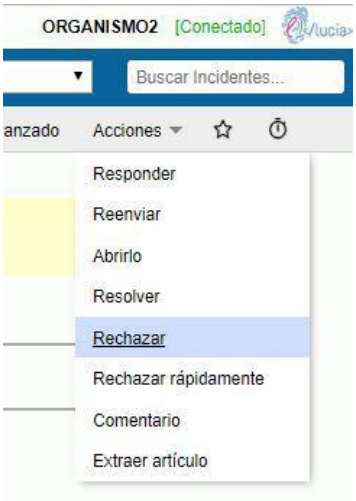
Si se necesita enlazar un reporte de incidente o una investigación a un incidente, hay que ir a la vista del ticket y editarlo. Se selecciona la opción 'Enlazar' y el o los tickets y se da a 'Enlazar'.



Par poder enlazar hay que ser propietario del ticket.

Rechazar y abandonar.

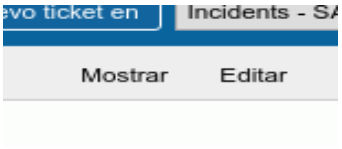
Un reporte de incidente se puedes rechazarlo de dos maneras diferentes ‘Rechazar’ y ‘Rechazar rápidamente’.



Con la opción rechazar se incluye información y envía un comentario o una respuesta para justificar el motivo del rechazo. Sin embargo, ‘Rechazar rápidamente’ el ticket no es necesario introducir una información que llegue al usuario.

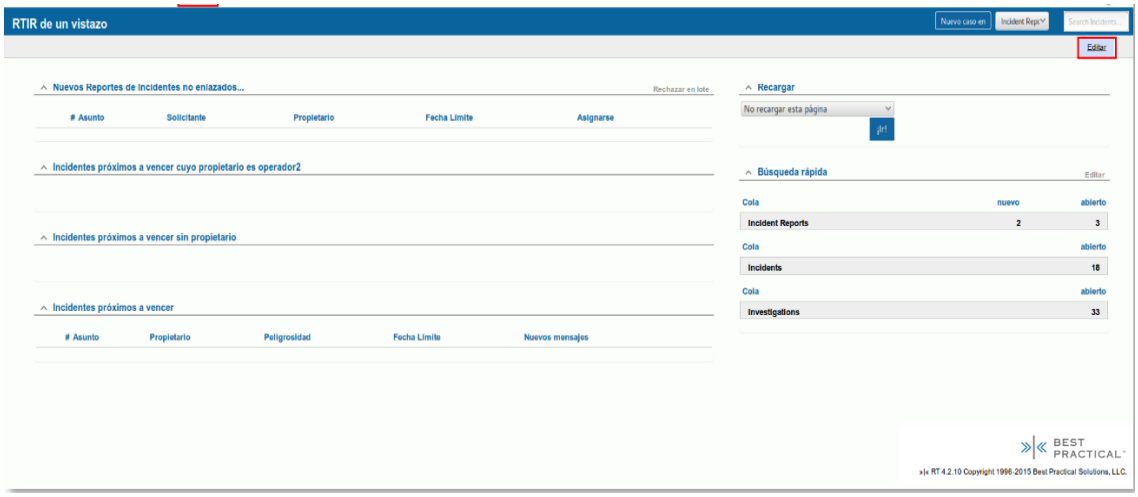
Borrar ticket.

Solo se puede borrar tickets propios. Para ello hay que situarse en la página ‘Mostrar’ del ticket y en el menú superior “Editar”.

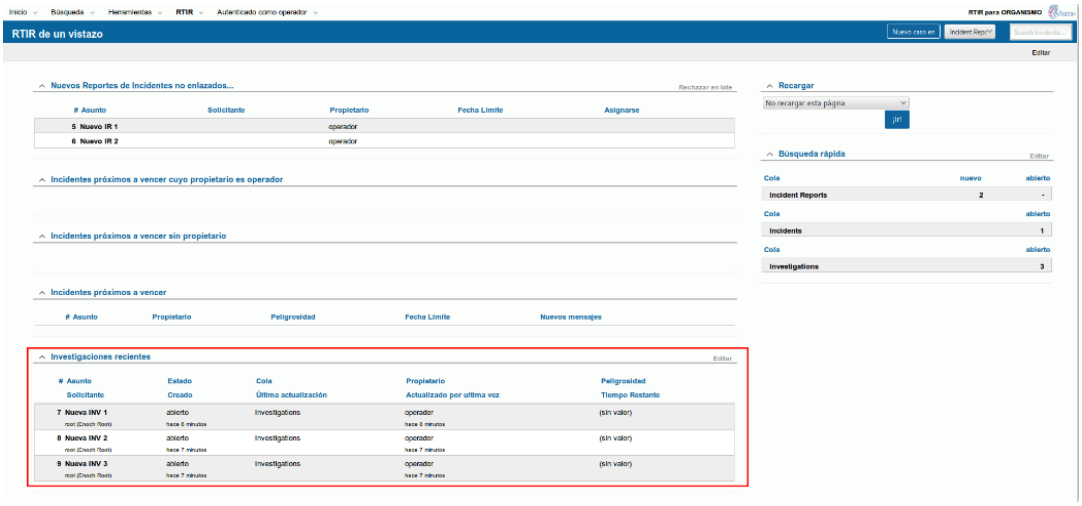


Personalizar paneles de RTIR.

Para personalizar se pulsa en *'RTIR'* y después a *'Editar'*:



Al personalizarlo aparecerá un nuevo panel con la búsqueda:



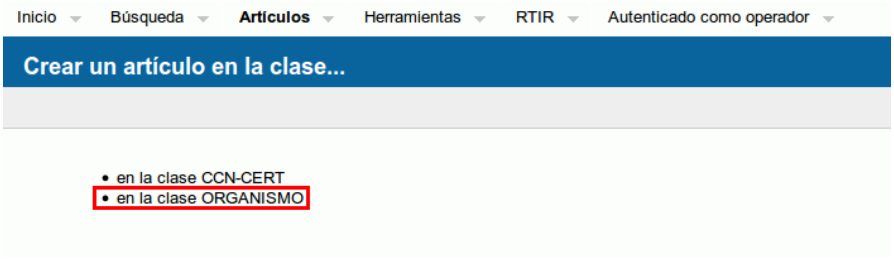
Artículos.

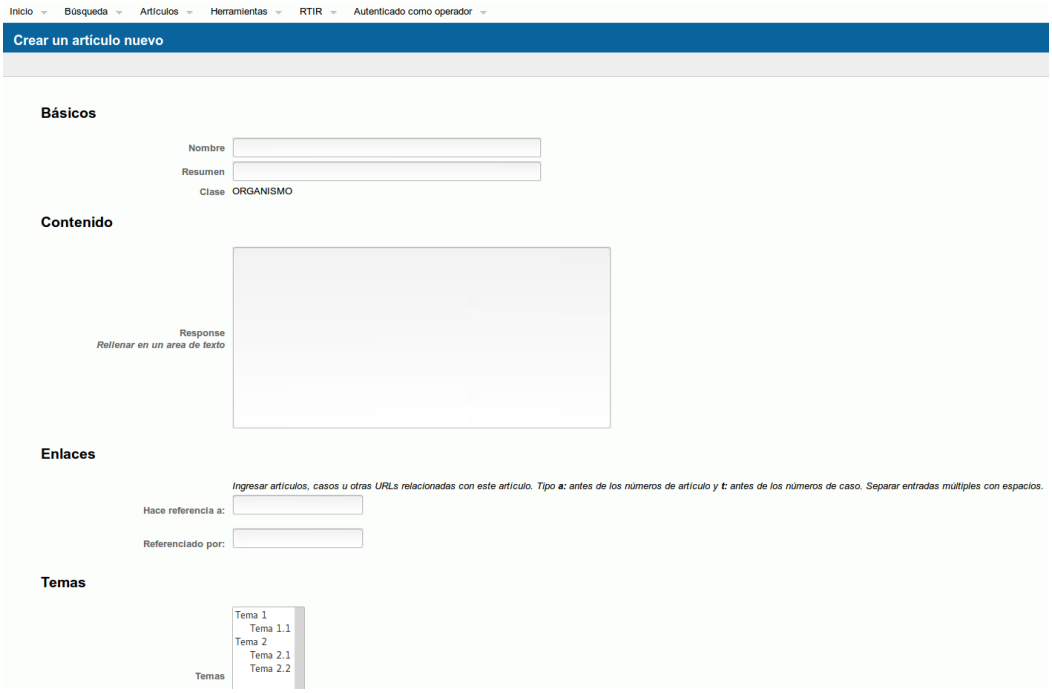
Es un texto predefinido a respuestas frecuentes. Así se añadirá a un incidente o comentarios rápidamente.

Crear un nuevo artículo.

Se crean desde *Artículos/crear*:

Se selecciona la clase donde se desea para crear y secrellenan los campos:



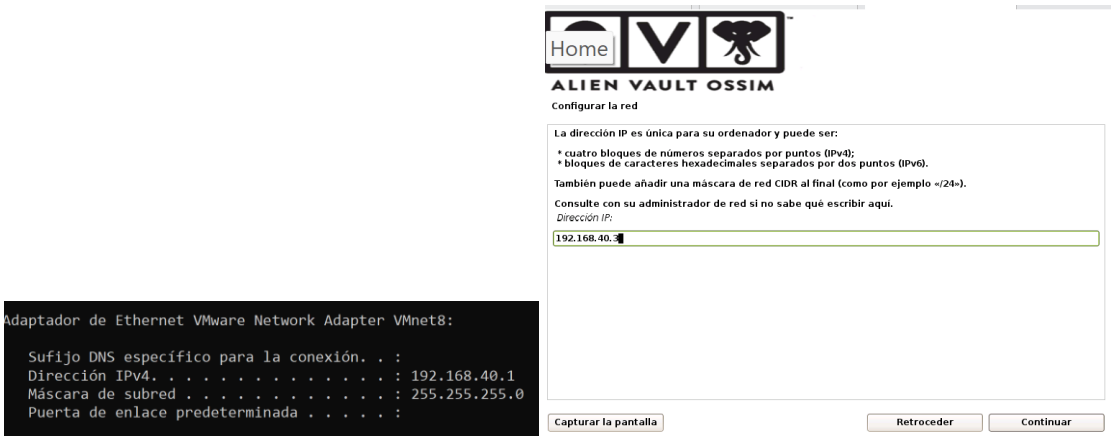


4.2 SIEM AlienVault.

Ahora se procederá a la instalación, configuración del SIEM de back-up o complementario de manera gratuita, aunque esté limitado en su versión libre. La versión gratuita tiene unas 85 reglas frente a las de más de 4.000 que aporta USM de pago.

Instalación: Se procede a descargar la ISO y montarla como máquina virtual con los siguientes requisitos:

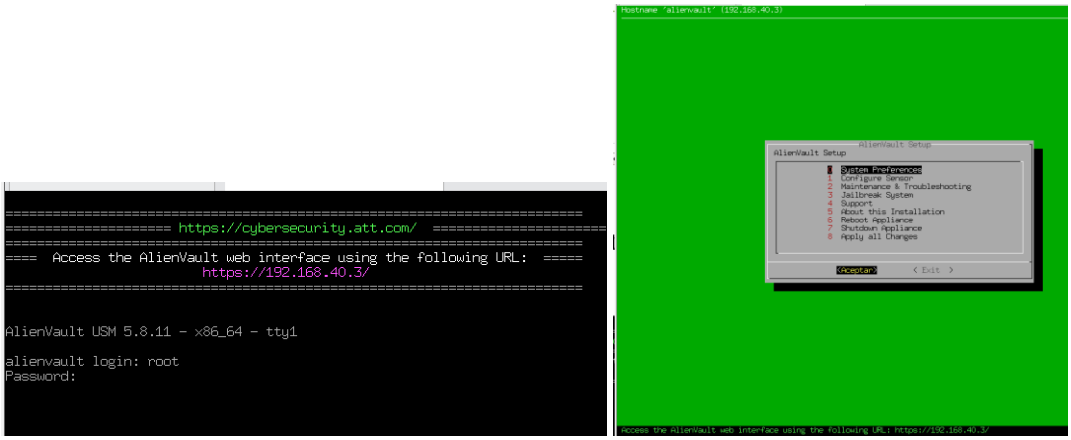
Se selecciona idioma,teclado y configuración regional en español. Se selecciona eth0 como interfaz de red principal y se introduce la configuración de red. Se recuerda que eth0 es NAT con lo cual la que de dentro del rango del NAT de Vmware, se añade máscara de subred, puerta de enlace y dns. Pedirá meter una contraseña y ya empieza la instalación:


Home
ALIEN VAULT OSSIM
Configurar la red
La dirección IP es única para su ordenador y puede ser:
* cuatro bloques de números separados por puntos (IPv4);
* bloques de caracteres hexadecimales separados por dos puntos (IPv6).
También puede añadir una máscara de red CIDR al final (como por ejemplo «/24»).
Consulte con su administrador de red si no sabe qué escribir aquí.
Dirección IP:
192.168.40.3
Capturar la pantalla
Retroceder
Continuar
Adaptador de Ethernet VMware Network Adapter VMnet8:
Sufijo DNS específico para la conexión. . :
Dirección IPv4. . . . . : 192.168.40.1
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . . . :

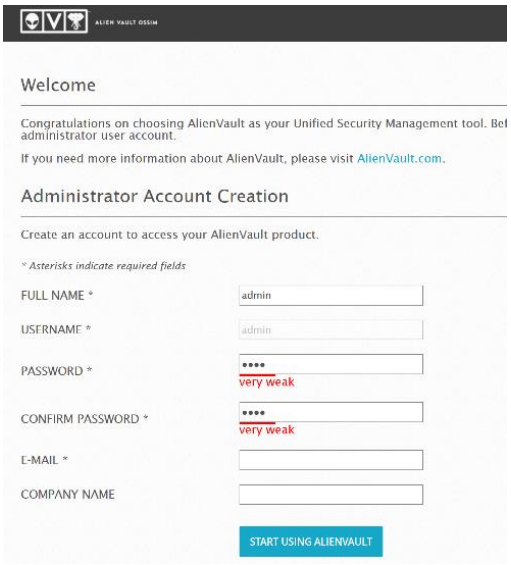

Home
ALIEN VAULT OSSIM
Configurar la red
La máscara de red se utiliza para determinar qué sistemas están incluidos en la red. Consulte al administrador de red si no conoce el valor. La máscara de red debería introducirse como cuatro números separados por puntos.
Máscara de red:
255.255.255.0
Capturar la pantalla
Retroceder
Continuar
ALIEN VAULT OSSIM
Configurar la red
La pasarela es una dirección IP (cuatro números separados por puntos) que indica el encaminador de pasarela, también conocido como encaminador por omisión. Todo el tráfico que se envía fuera de su LAN (por ejemplo, hacia Internet) se envía a este encaminador. En algunas circunstancias anormales, puede no tener un encaminador; si es así lo puede dejar en blanco. Si no sabe la respuesta correcta a esta pregunta, consulte al administrador de red.
Pasarela:
192.168.40.1
Capturar la pantalla
Retroceder
Continuar

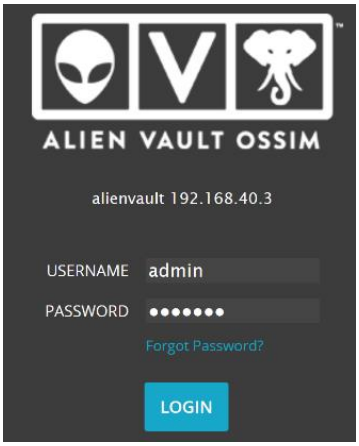

ALIEN VAULT OSSIM
Configurar la red
Los servidores de nombres se utilizan para buscar los nombres de las máquinas de la red. Por favor, introduzca la dirección IP (no el nombre de sistema) de hasta tres servidores de nombres, separados por espacios. No utilice comas. Se consultarán los servidores en el orden en que se introduzcan. Si no quiere utilizar ningún servidor de nombres deje este campo en blanco.
Direcciones de servidores de nombres:
192.168.40.1
Capturar la pantalla
Retroceder
Continuar
ALIEN VAULT OSSIM
Configurar usuarios y contraseñas
sistema. Podría tener graves consecuencias que un usuario malicioso o un usuario sin la debida cualificación tuviera acceso a la cuenta del administrador del sistema, así que debe tener cuidado y elegir un la contraseña para el superusuario que no sea fácil de adivinar. No debería ser una palabra que se encuentre en el diccionario, o una palabra que pueda asociarse fácilmente con usted.
Una buena contraseña debe contener una mezcla de letras, números y signos de puntuación, y debe cambiarse regularmente.
La contraseña del usuario «root» (administrador) no debería estar en blanco. Si deja este valor en blanco, entonces se deshabilitará la cuenta de root creará una cuenta de usuario a la que se le darán permisos para convertirse en usuario administrador utilizando la orden «sudo».
Tenga en cuenta que no podrá ver la contraseña mientras la introduce.
Clave del superusuario:
Mostrar la contraseña en claro
Por favor, introduzca la misma contraseña de superusuario de nuevo para verificar que la introdujo correctamente.
Vuelva a introducir la contraseña para su verificación:
Mostrar la contraseña en claro
Capturar la pantalla
Retroceder
Continuar

Se ejecuta y se introducen credenciales para ver que está instalado:

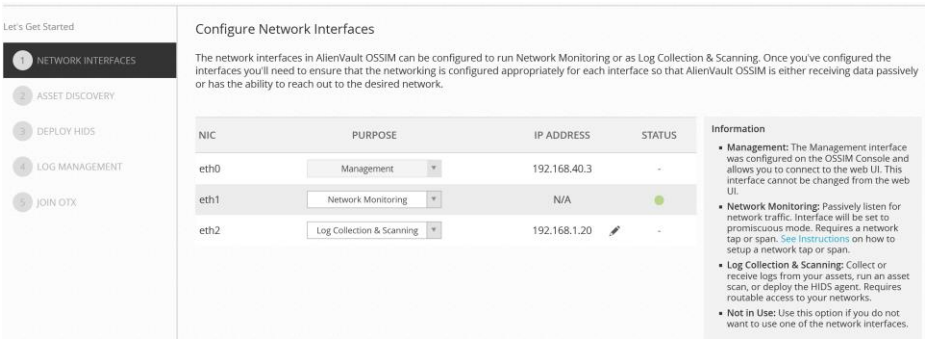


Ahora desde navegador se introduce la IP: 192.168.40.3 y se registra usuario admin:

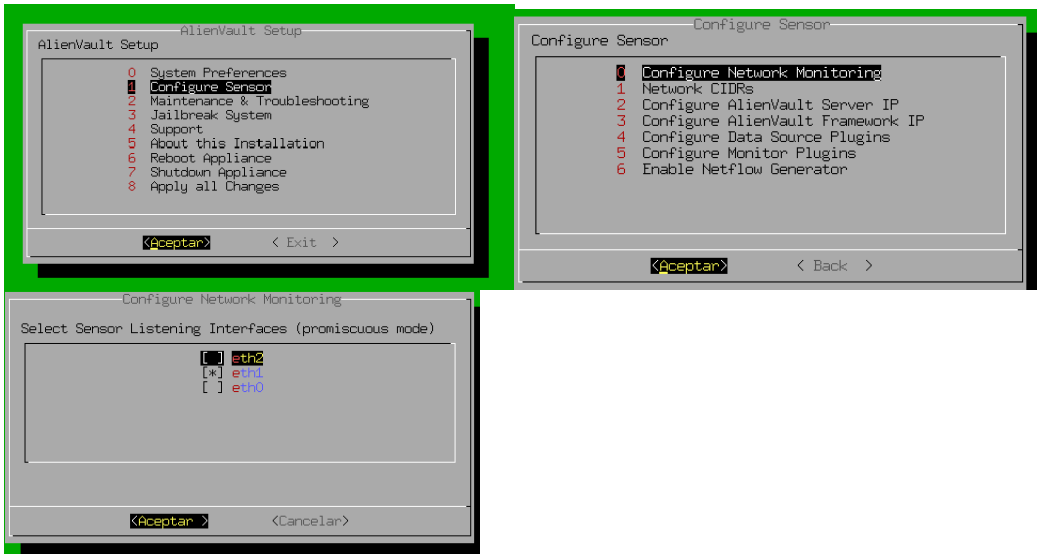




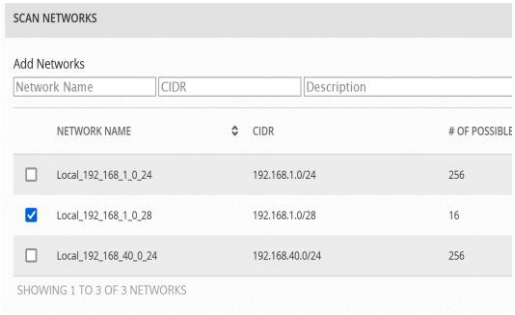
Ahora se procede a la configuración de interfaz de red, eth0 para acceder a la interfaz web, network monitoring en eth1 y en eth2 con IP bridge de red local.

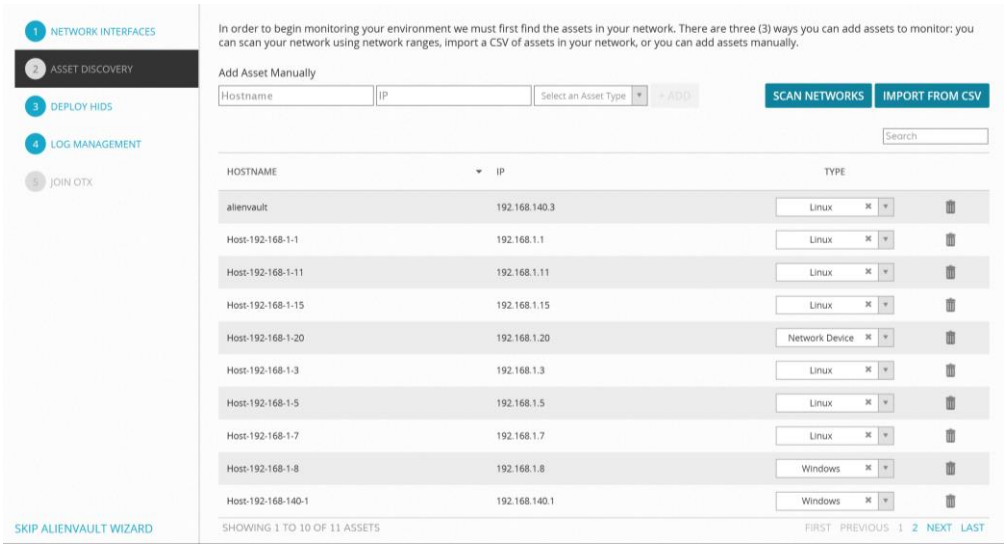


Para habilitar la función de Network Monitoring se entra en la consola en la opción de configure sensor y seleccionar la interfaz de red eth1:

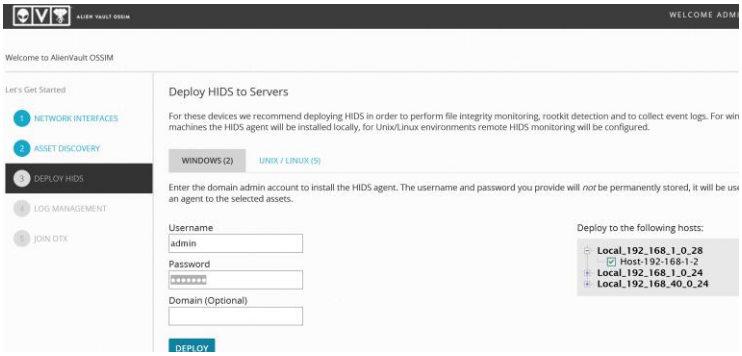


Ahora se va a escanear la red o añadir manualmente los asset que se quiere monitorizar. En este caso se realiza un scan manual de la red local y acotada para que no tarde demasiado y se ven los resultados:

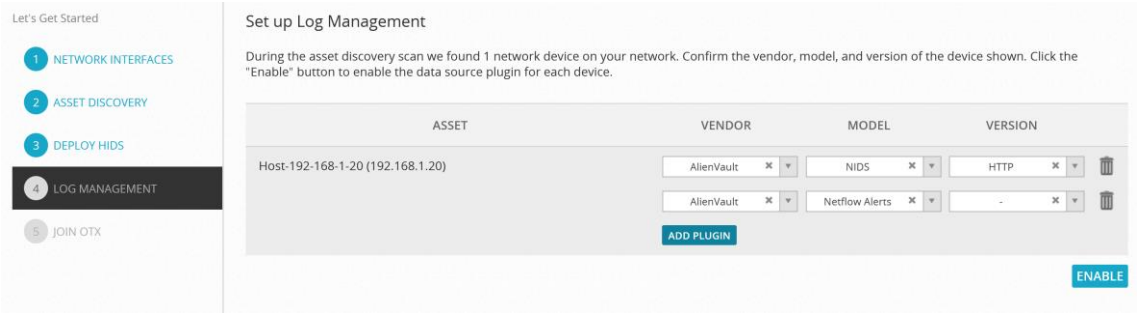




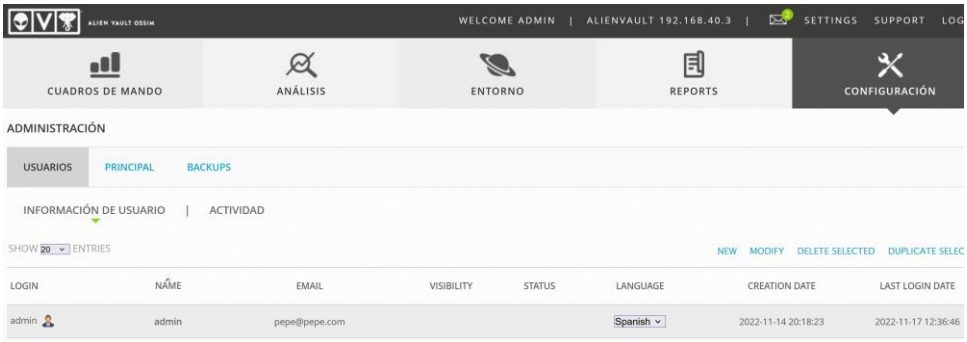
Ahora se reliza el despliegue de los agentes de host HIDS para los asset que se quieran. En este caso se desplegarán en el anfitrión con windows 11.



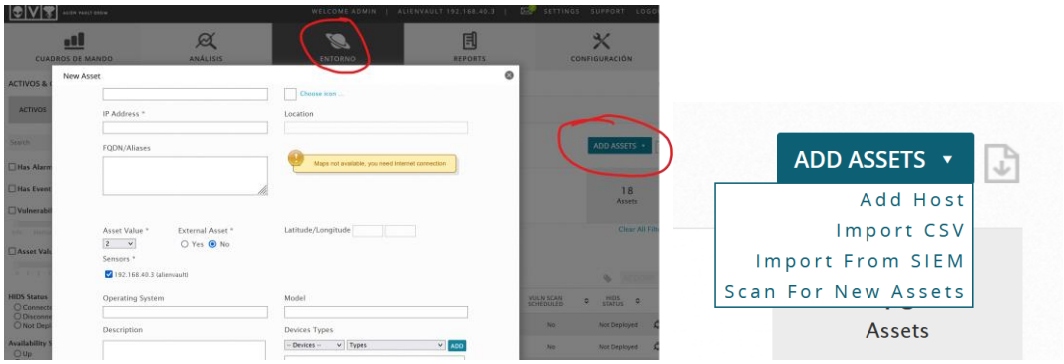
Se configura la interfaz de red para el log collectión:



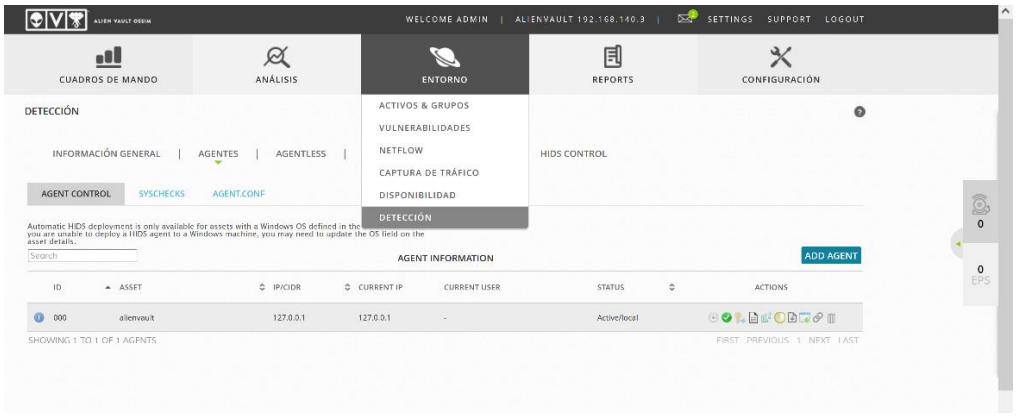
Más adelante se configuran manualmente los HIDS. Con esto se finalizan todas las opciones y se va al menú principal para cambiar idioma a español:

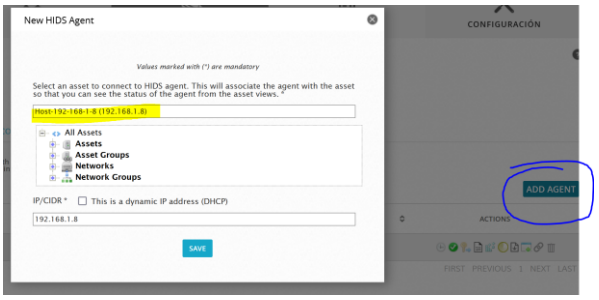


Aquí también se puedes añadir a más usuarios. Si se necesita añadir un activo más, en la pestaña de entornos/activos y añadir un activo de múltiples maneras:

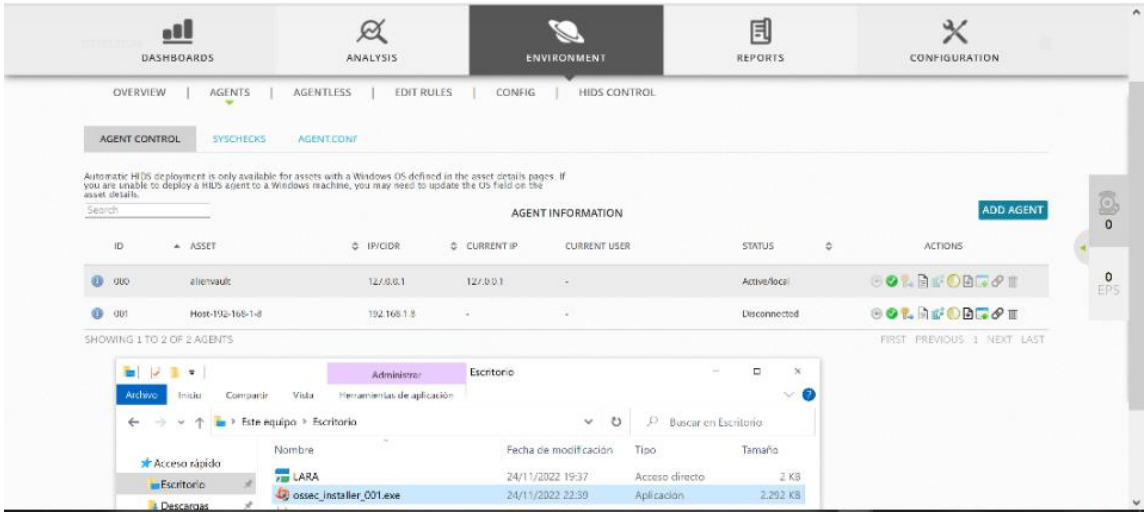


Para detectar eventos de Host, se instalas el agente en el host Windows, con lo cual se va a entorno/detección y sección de agentes para añadirlo nuevo:

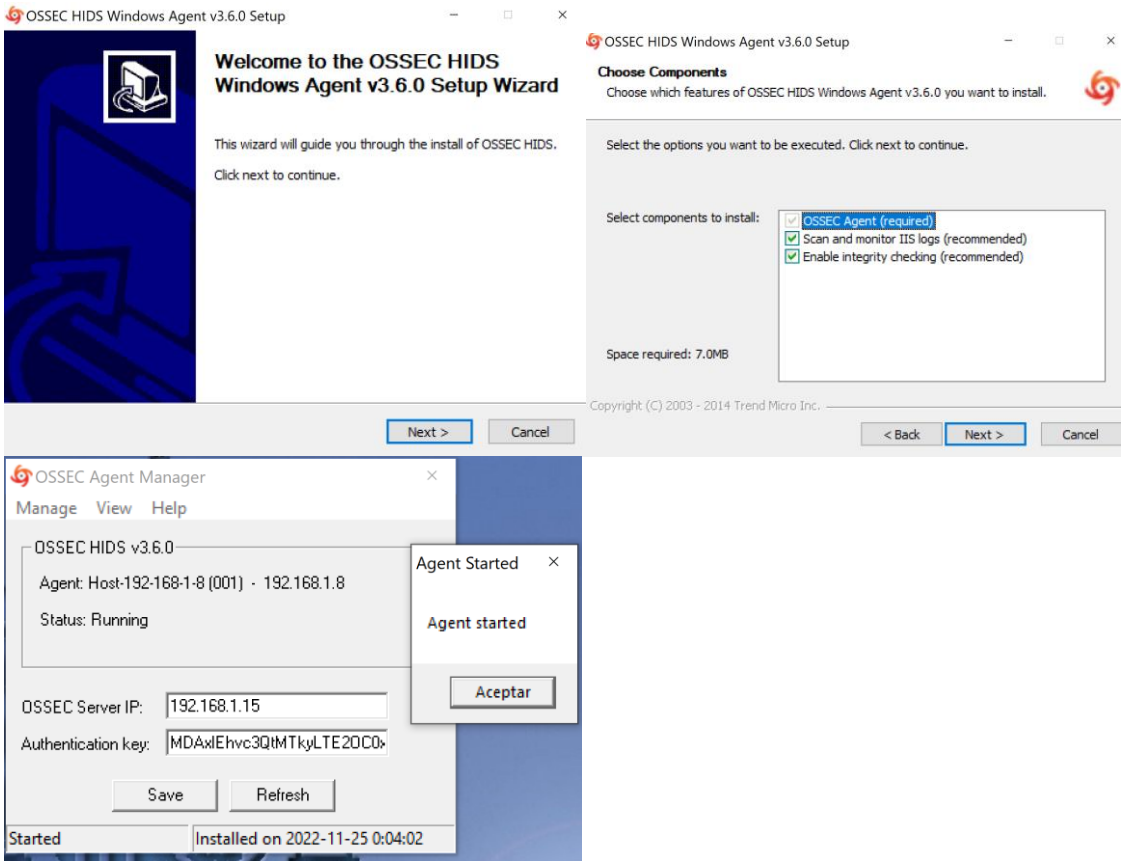




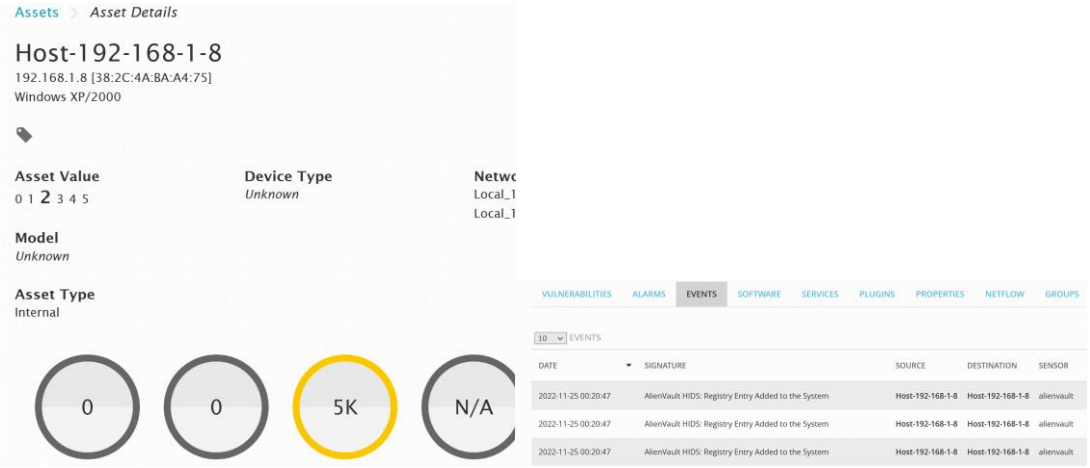
Se genera el cliente ossec y se instala en el host con Windows:



Se procede a su instalación:

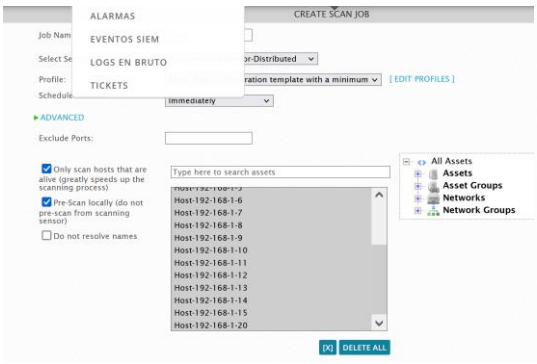


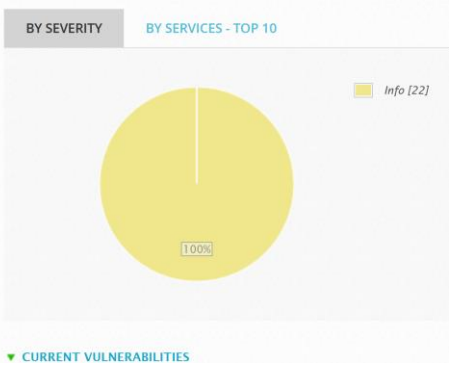
Para comprobar el HIDS se va a entorno/activos y se comprueba en el host con Windows si funciona viendo los eventos:

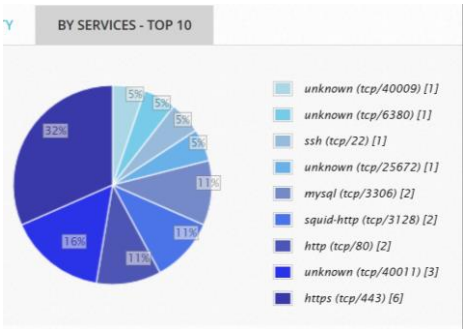


Si se comprueba un evento, se ve que el HIDS funciona e indica que se ha instalado un programa ya que detecta cambios en las clves de registro:

Se puede crear una lista de activos de red en la que se realiza un escaneo de vulnerabilidades con Openvas:

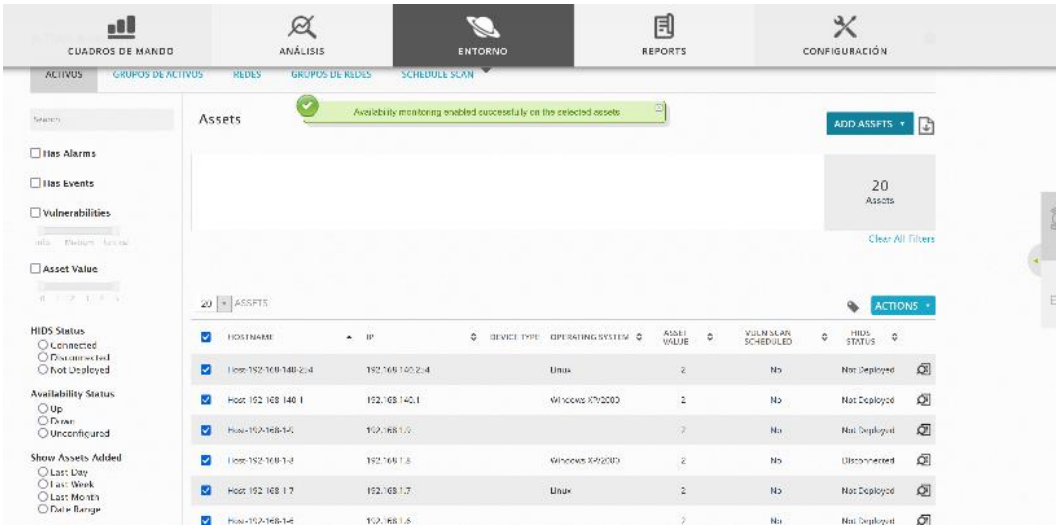


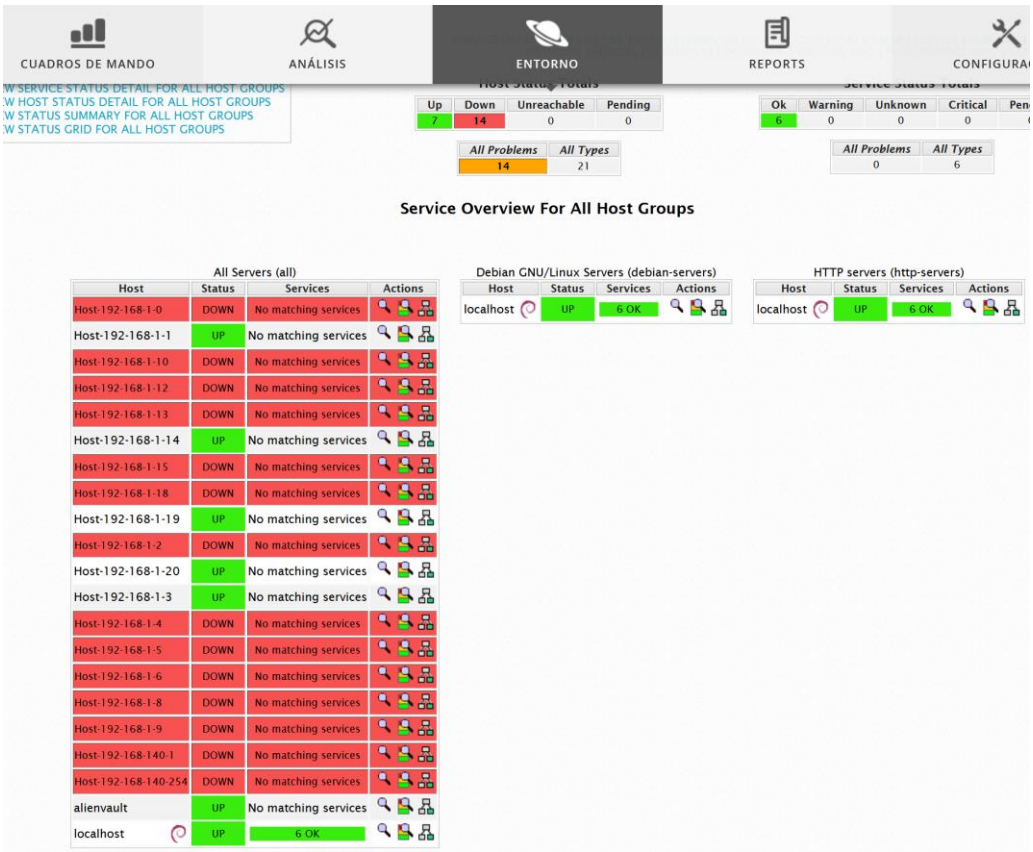




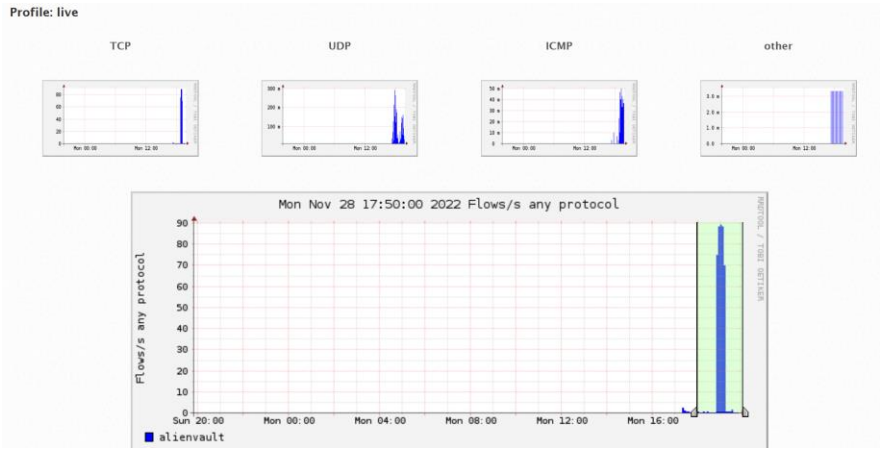
JOB NAME	LAUNCH TIME	SCAN START TIME	SCAN END TIME	SCAN TIME	NEXT SCAN	REPORTS
vuln2	2022-11-28 18:49:11	2022-11-28 18:50:02	2022-11-28 19:14:33	24 mins	-	(22)

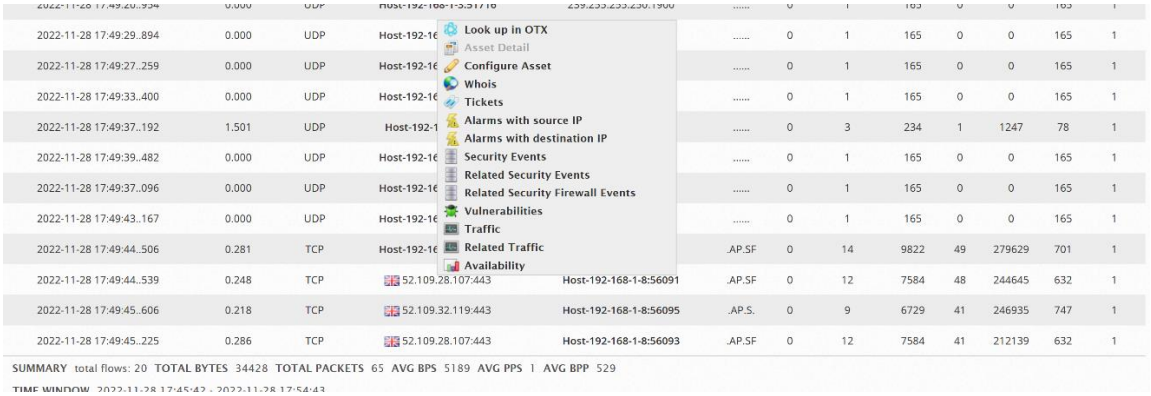
Se puede en entorno/activos seleccionar todos y activar la monitorización de disponibilidad:



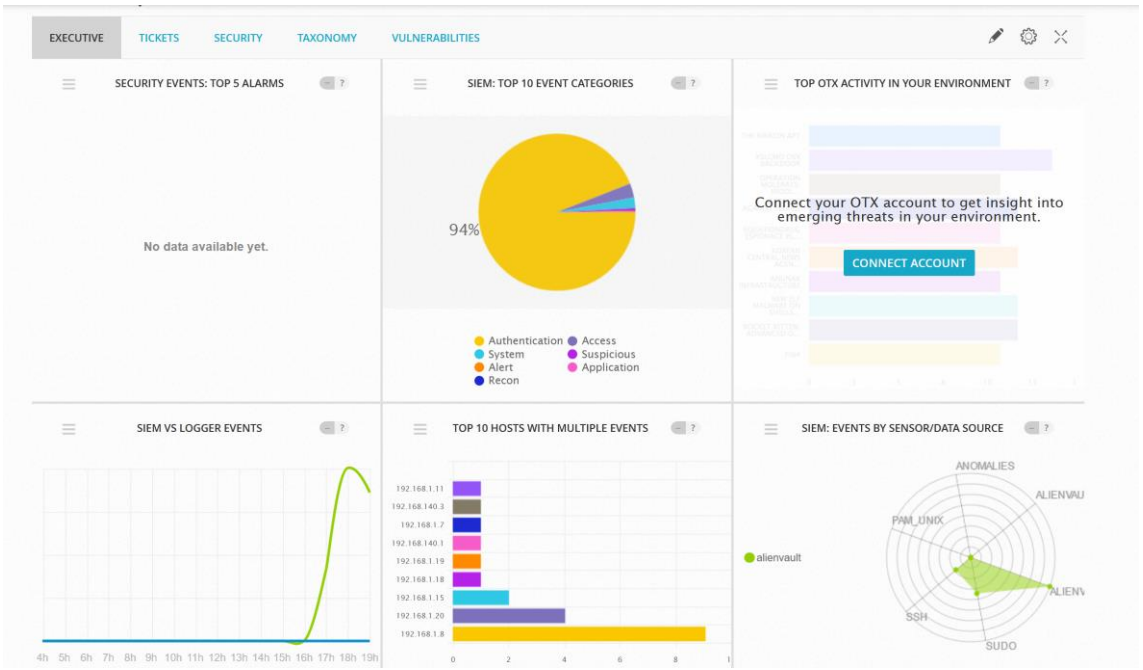


En el apartado NETFLOW se puede recoger información de tráfico de red por puertos y utilizar las herramientas para averiguar más información:

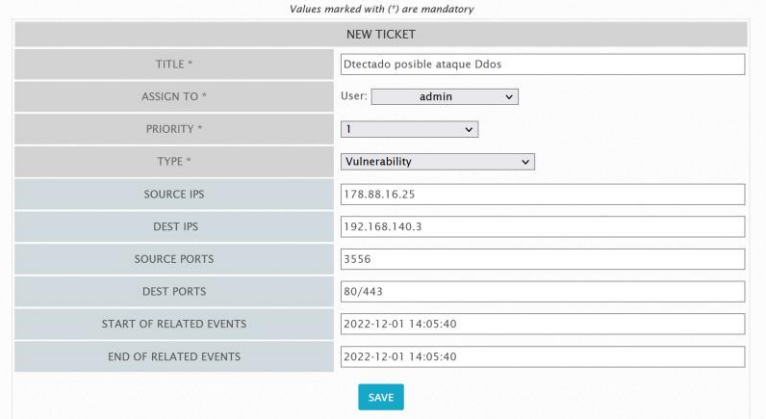




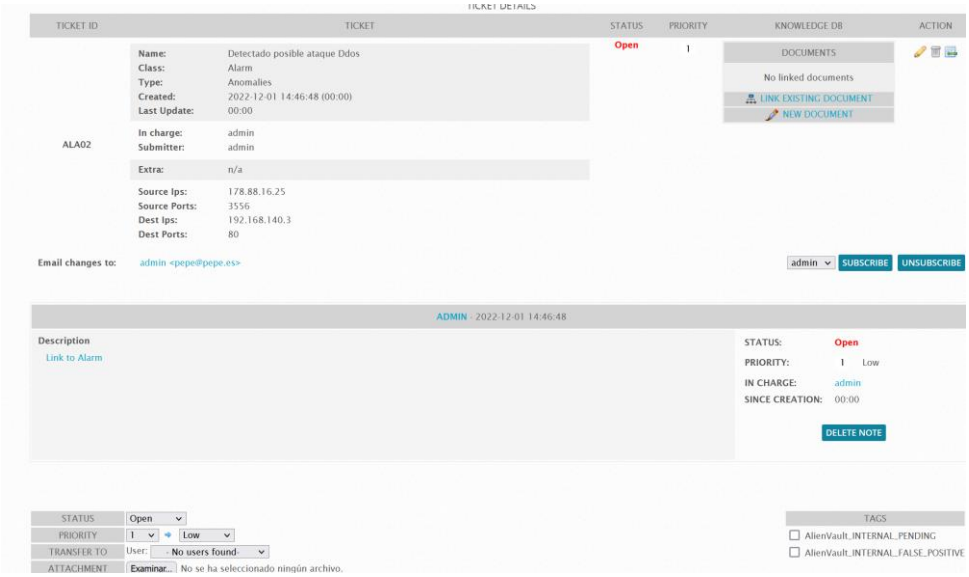
En la primera pestaña aparece los dashboard para informar del estado de la red y sirve como herramienta de ciberconciencia situacional:



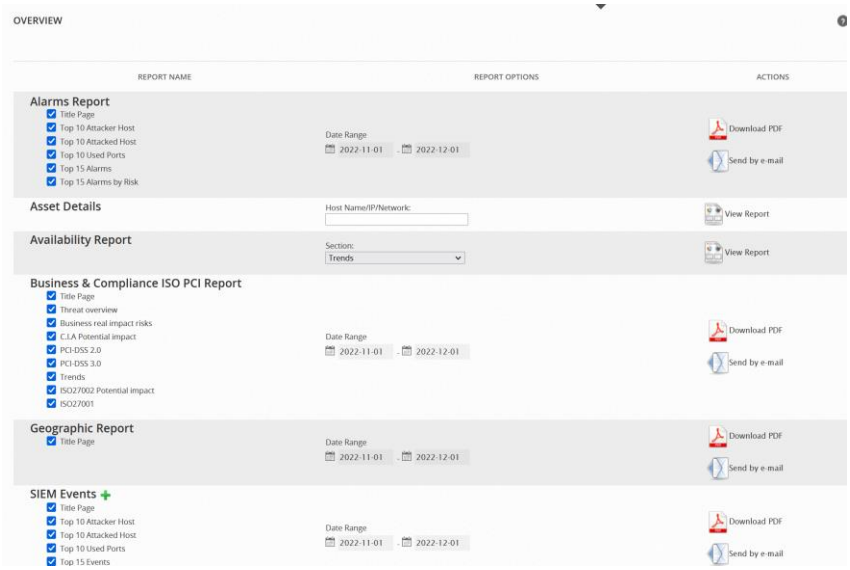
Tiene integrada su propia plataforma de Ticketing para incidentes:



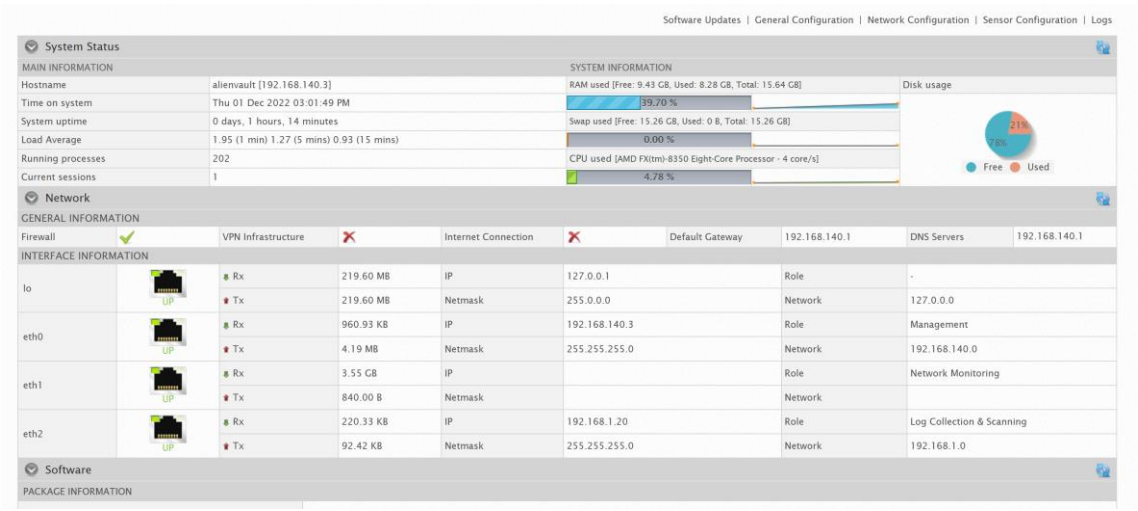
Aquí se podría editar el incidente, añadir comentarios, adjuntos para la investigación:



Como otro SIEM más incorpora la utilidad de generar informes:



En el apartado de configuración y despliegue se ve el sensor y las capacidades, almacenamiento…etc:



4.3 SIEM Security Onion.

Ya se ha comentado en capítulos anteriores las herramientas que integra: CyberChef, Elasticsearch, Logstash, Kibana, Suricata, Zeek, Wazuh…etc. Esta herramienta open source recogerá y analizará tráfico de red, eventos de host, almacenamiento de estos logs gracias a ELK y como no, poder interpretar estos logs con herramientas de visualización gráfica.

El producto ELK es un conjunto de 4 herramientas: Elasticsearch, logtash, Kibana y Beats. Estas herramientas permiten una centralización de logs, se podrá recolectar logs de diferentes fuentes, procesarlas y normalizarlas, almacenarlas durante un periodo de tiempo y su posterior análisis.

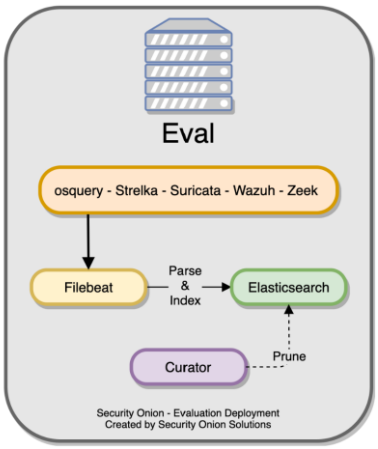
Hay diferentes tipos de arquitecturas disponibles, hay que centrarse en la de: import, evaluation, standalone y distributed. Se va a explicar las diferentes arquitecturas:

Import

Es la arquitectura más fácil y sencilla. Solo es necesario un único nodo para el capturador de paquetes. Cuando se captura tráfico de la red, Suricata y Zeek se analizan los paquetes y la generación de logs que son recolectados por Filebeat y posteriormente enviados a ElasticSearch.

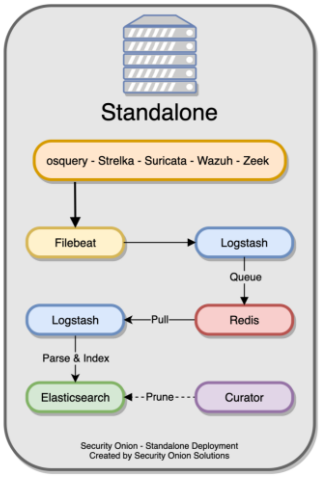
Evaluation

Para esta arquitectura se tiene que tener una interfaz de red para obtener el tráfico a través de un span port. Éste es una interfaz de red física o simulada por software para procesar y guardar el tráfico de red en tiempo real.



Standalone

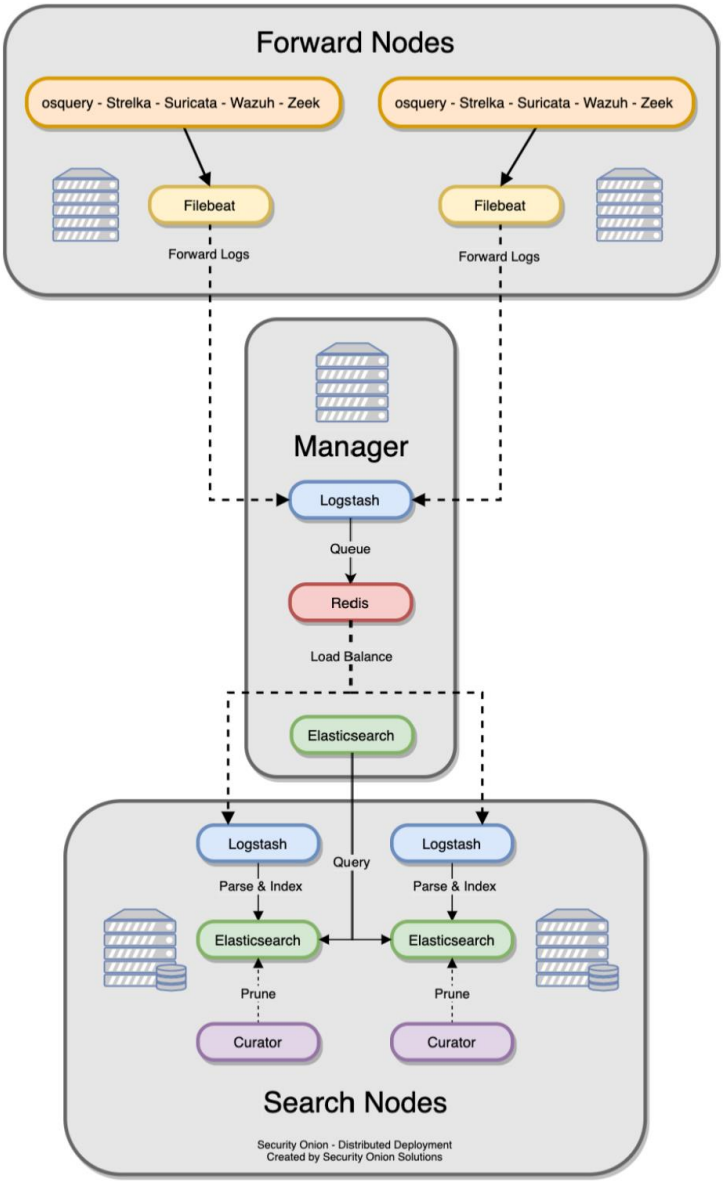
Es parecida a evaluation en la forma de obtener logs. Sin embargo, éstos se dirigirán primero a Logstash para tratarlos después con Elasticsearch. Logstash actuará en este caso dos veces para obtener logs de la cola y enviárselos a ElasticSearch.



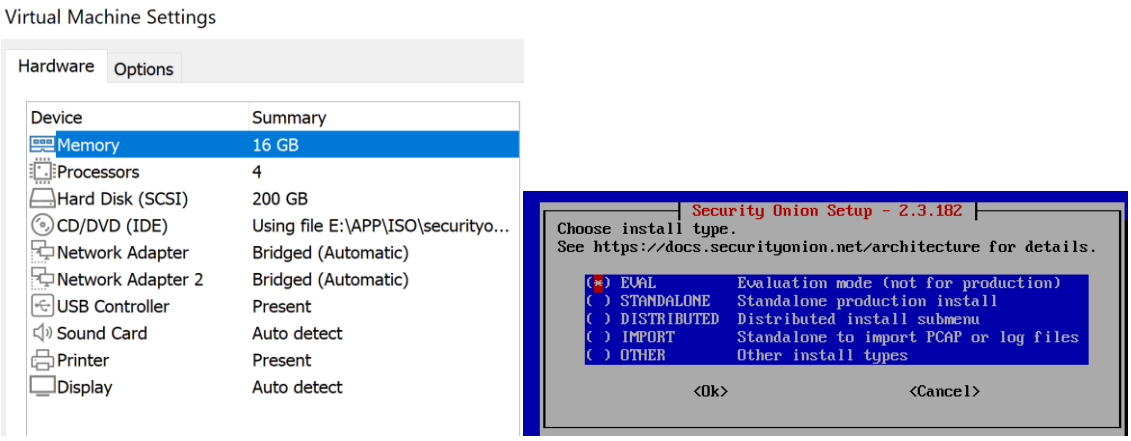
Distribuida

Esta se basa en la división de las funciones en diferentes nodos. Se aumenta el coste, pero se garantiza una mayor escalabilidad y rendimiento. Hay 3 tipos de nodos:

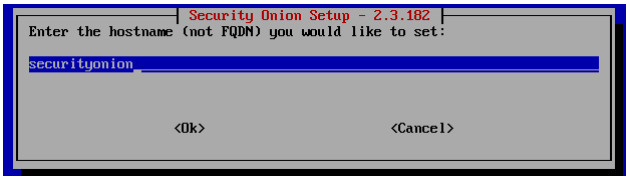
- Nodos forward: Para la obtención de logs usarán los IDS de la red. A continuación, los logs se enviarán mediante Filebeat.
- Manager. Elasticsearch y Redis se encargarán de hacer las colas de logs y el balance de carga entre los distintos Search Nodes.
- Nodos search. Sobre ElasticSearch en instancia local se obtienen logs de la cola para indexar y almacenar.

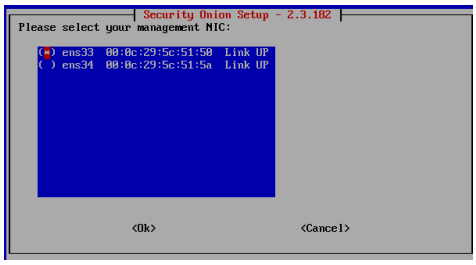


Se procede a instalar Security Onion, modo evaluación. Se descarga su ISO en este caso la versión 2.3.182 de la web oficial y se monta en máquina virtual con hypersivor Vmware pro con la siguiente configuración adecuándose a los requisitos mínimos e instalarse con la primera opción:

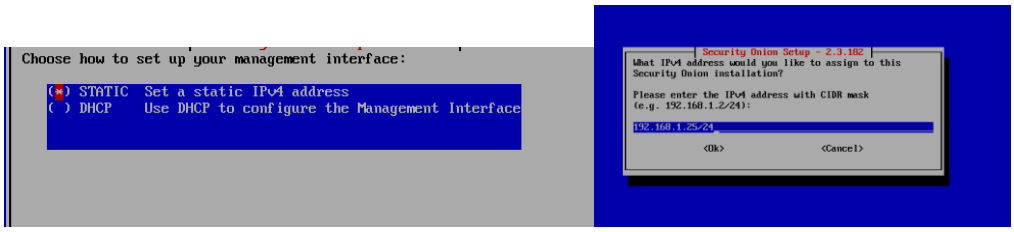


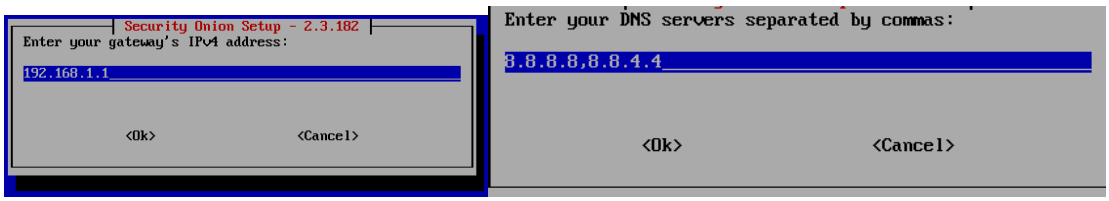
Al terminarse la instalación se reinicia pidiendo usuario y contraseña. A continuación, se procede a la configuración con los siguientes pasos. Se selecciona modo evaluación si es la primera vez que lo se va a testear como se indica en su web y debido a las características hardware. Evidentemente para un entorno empresarial, se realizaría la instalación en modo distribuido con varios nodos.

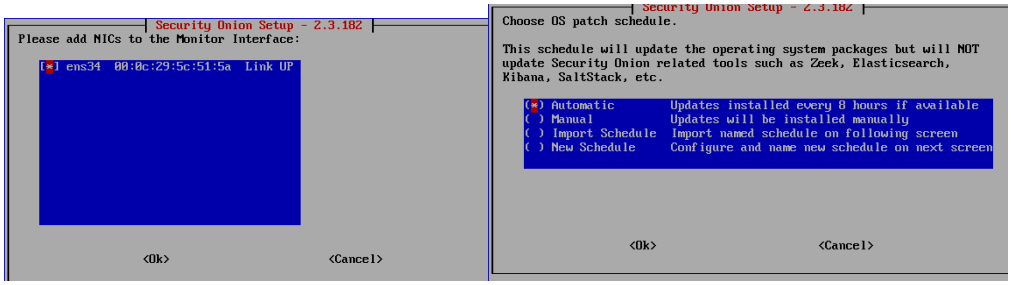


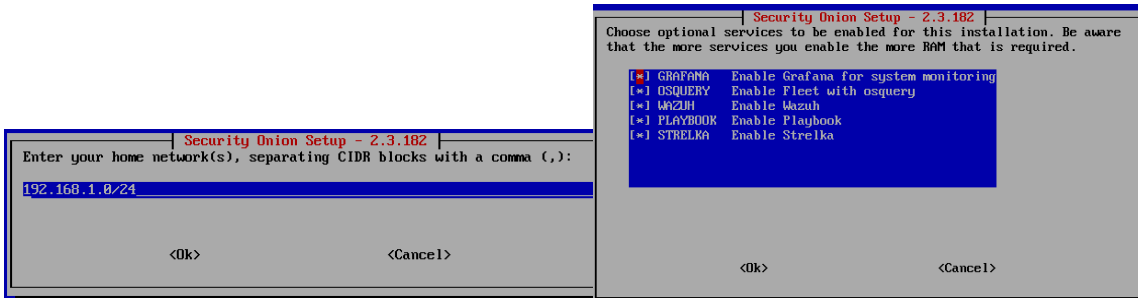


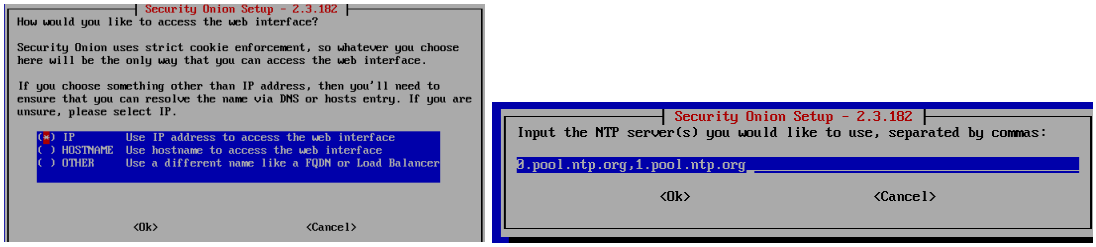
Se selecciona la primera interfaz de red de las dos que aparecen ya que la segunda será para la monitorización de red.


Choose how to set up your management interface:
(*) STATIC Set a static IPv4 address
( ) DHCP Use DHCP to configure the Management Interface
Security Onion Setup - 2.3.182
What IPv4 address would you like to assign to this Security Onion installation?
Please enter the IPv4 address with CIDR mask (e.g. 192.168.1.2/24):
192.168.1.25/24
<Ok>
<Cancel>

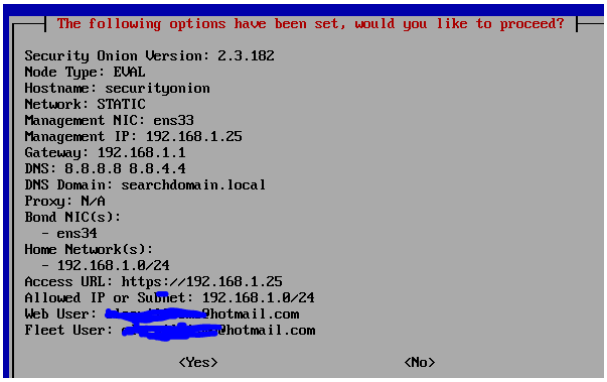

Security Onion Setup - 2.3.182
Enter your gateway's IPv4 address:
192.168.1.1
<Ok>
<Cancel>
Enter your DNS servers separated by commas:
8.8.8.8,8.8.4.4
<Ok>
<Cancel>


Security Onion Setup - 2.3.182
Please add NICs to the Monitor Interface:
[*] ens34 00:0c:29:5c:51:5a Link UP
<Ok>
<Cancel>
Security Onion Setup - 2.3.182
Choose OS patch schedule.
This schedule will update the operating system packages but will NOT update Security Onion related tools such as Zeek, Elasticsearch, Kibana, SaltStack, etc.
(*) Automatic Updates installed every 8 hours if available
( ) Manual Updates will be installed manually
( ) Import Schedule Import named schedule on following screen
( ) New Schedule Configure and name new schedule on next screen
<Ok>
<Cancel>

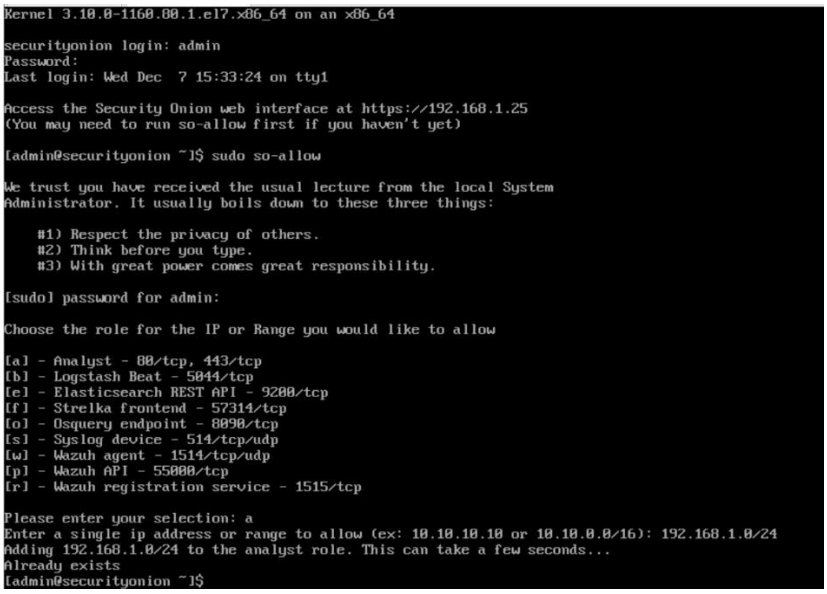

Security Onion Setup - 2.3.182
Enter your home network(s), separating CIDR blocks with a comma (,):
192.168.1.0/24
<Ok>
<Cancel>
Security Onion Setup - 2.3.182
Choose optional services to be enabled for this installation. Be aware that the more services you enable the more RAM that is required.
[*] GRAFANA Enable Grafana for system monitoring
[*] OSQUERY Enable Fleet with osquery
[*] WAZUH Enable Wazuh
[*] PLAYBOOK Enable Playbook
[*] STRELKA Enable Strelka
<Ok>
<Cancel>


Security Onion Setup - 2.3.182
How would you like to access the web interface?
Security Onion uses strict cookie enforcement, so whatever you choose here will be the only way that you can access the web interface.
If you choose something other than IP address, then you'll need to ensure that you can resolve the name via DNS or hosts entry. If you are unsure, please select IP.
(*) IP Use IP address to access the web interface
( ) HOSTNAME Use hostname to access the web interface
( ) OTHER Use a different name like a FQDN or Load Balancer
<Ok>
<Cancel>
Security Onion Setup - 2.3.182
Input the NTP server(s) you would like to use, separated by commas:
0.pool.ntp.org,1.pool.ntp.org
<Ok>
<Cancel>

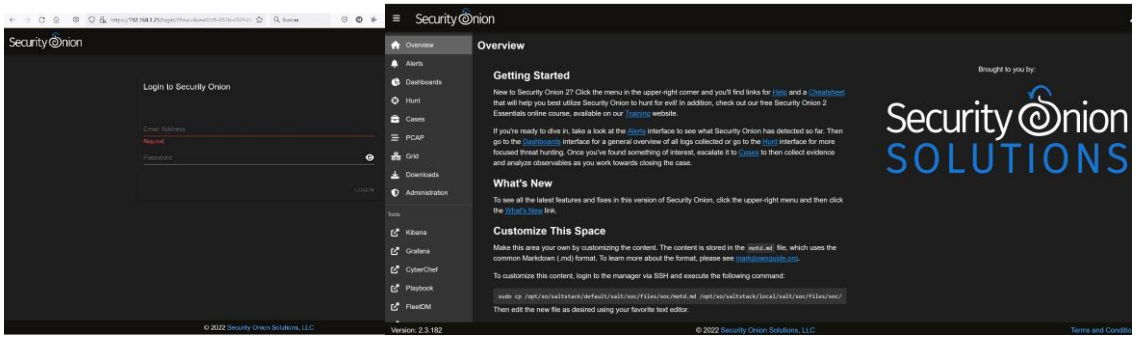
Se sigue con todas las opciones por defecto y se termina con un resumen:



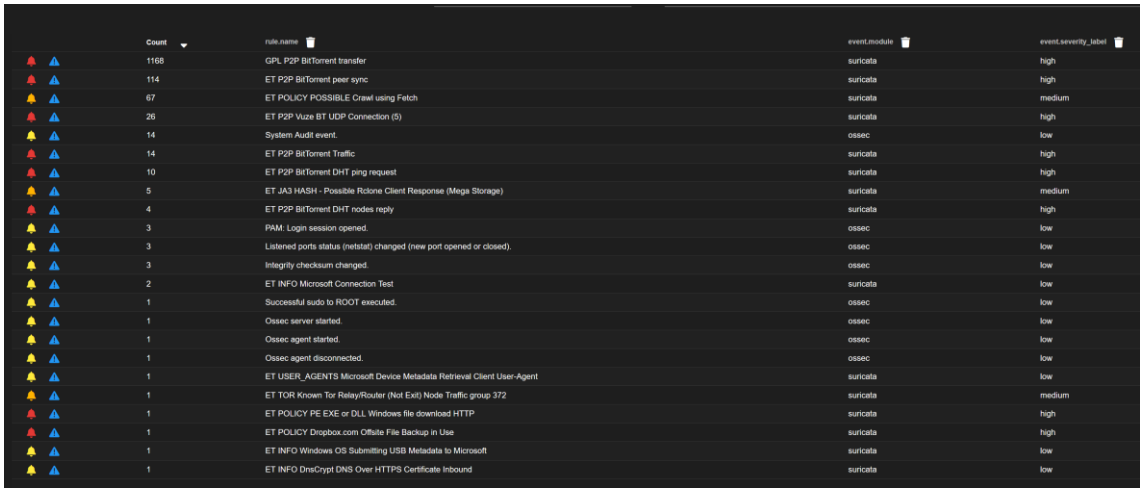
Se verifica que todo está correcto y al finalizar la instalación, se abre el navegador y antes de meter IP se autoriza vía consola el rango local con el comando so-allow, ya que se tiene la interfaz de red en bridge para que se pueda acceder desde cualquier dispositivo de la red local.



Ahora ya salta la interfaz y se accede a la pantalla principal:

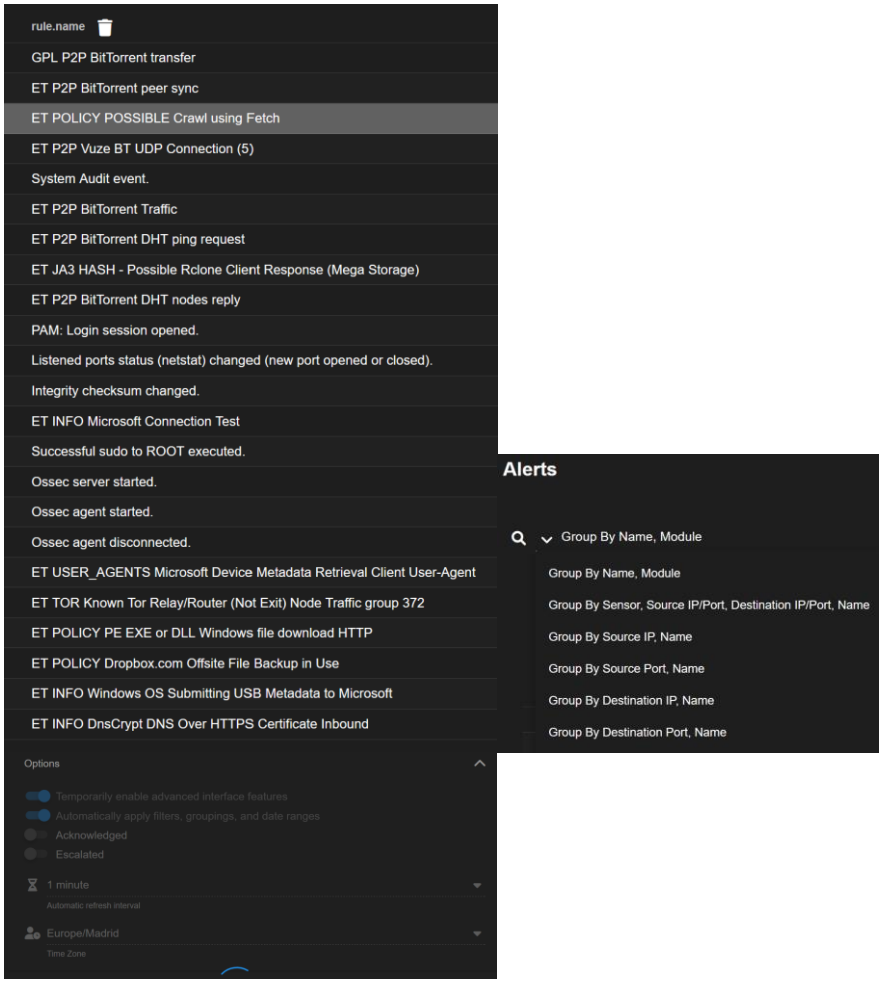


En la primera ventana de Alerts, aparecerá alertas de NIDS provenientes de suricata y de HIDS proveniente de Ossec.

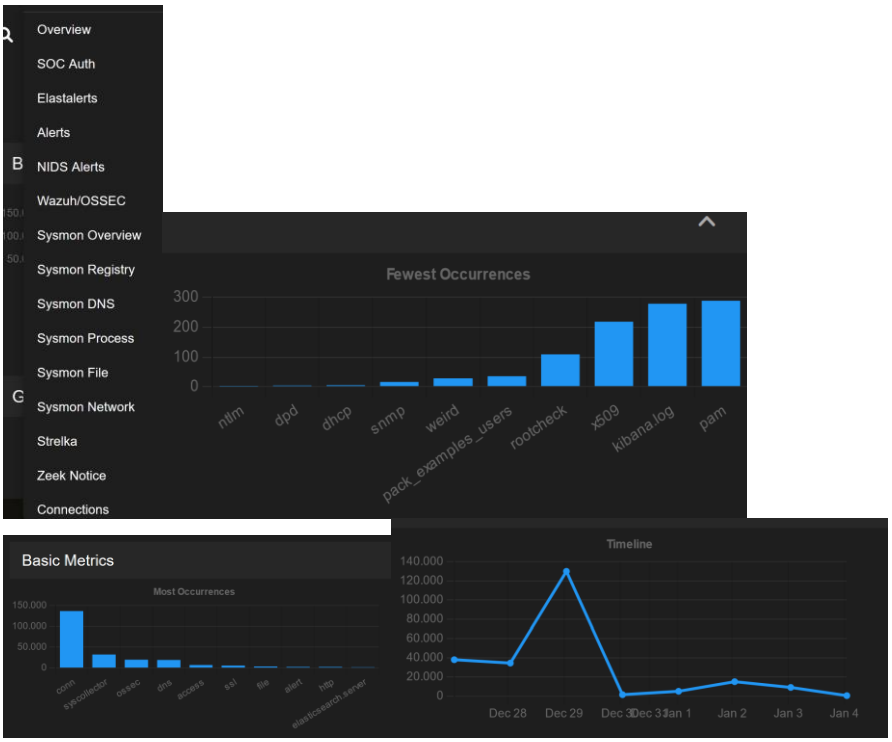


Count	rule.name	event.module	event.severity_label
1168	GPL P2P BitTorrent transfer	suricata	high
114	ET P2P BitTorrent peer sync	suricata	high
67	ET POLICY POSSIBLE Crawl using Fetch	suricata	medium
26	ET P2P Vuze BT UDP Connection (5)	suricata	high
14	System Audit event.	ossec	low
14	ET P2P BitTorrent Traffic	suricata	high
10	ET P2P BitTorrent DHT ping request	suricata	high
5	ET JA3 HASH - Possible Rclone Client Response (Mega Storage)	suricata	medium
4	ET P2P BitTorrent DHT nodes reply	suricata	high
3	PAM: Login session opened.	ossec	low
3	Listened ports status (netstat) changed (new port opened or closed).	ossec	low
3	Integrity checksum changed.	ossec	low
2	ET INFO Microsoft Connection Test	suricata	low
1	Successful sudo to ROOT executed.	ossec	low
1	Ossec server started.	ossec	low
1	Ossec agent started.	ossec	low
1	Ossec agent disconnected.	ossec	low
1	ET USER_AGENTS Microsoft Device Metadata Retrieval Client User-Agent	suricata	low
1	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 372	suricata	medium
1	ET POLICY PE EXE or DLL Windows file download HTTP	suricata	high
1	ET POLICY Dropbox.com Offsite File Backup in Use	suricata	high
1	ET INFO Windows OS Submitting USB Metadata to Microsoft	suricata	low
1	ET INFO DnsCrypt DNS Over HTTPS Certificate Inbound	suricata	low

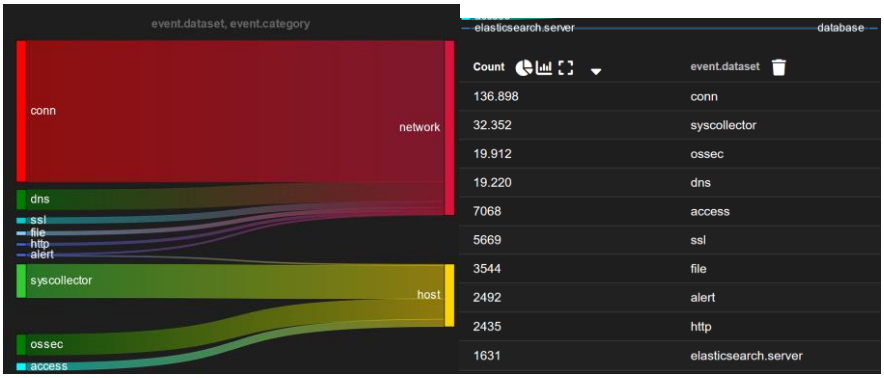
Ejemplo de alertas de Suricata y Ossec. Estas alertas se pueden agrupar y filtrar por tiempo. Se podrá habilitar más características con las opciones:



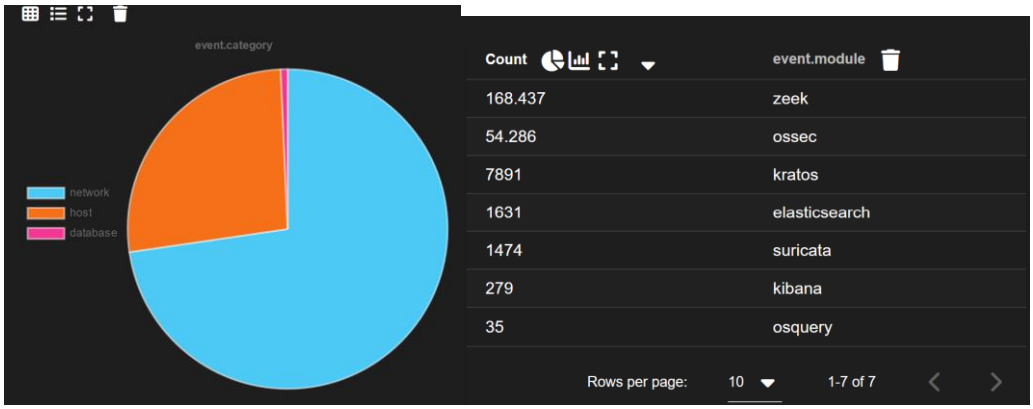
En el apartado Dashboards se ve no solo las alertas de HIDS/NIDS sino también de logs de Zeek, Suricata y cualquiera otra fuente recolectara de logs que se tenga. Este apartado es la herramienta de ciber conciencia situacional. De un vistazo se puede interpretar los datos y ver el estado de salud de la red. Primeramente, se tiene 3 métricas que se puede elegir las que se quiera a través de un filtro:

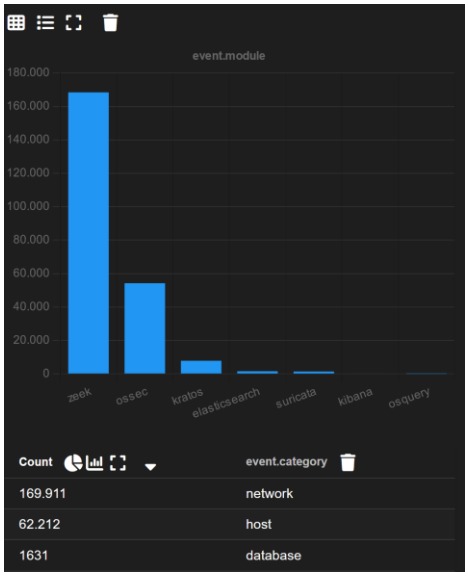


Se ve por defecto 10 valores de mayores sucesos, barra del tiempo y los 10 sucesos (reglas IDS) más repetidos. Ahora se verán los grupos de métricas, son personalizables que permiten añadir campos arbitrarios. La visualización gráfica puede configurarse en barras, sectorial ...etc.

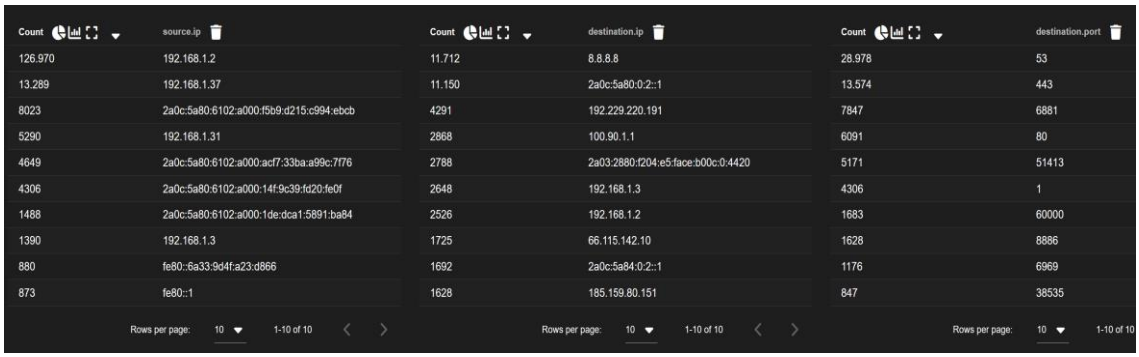


En la primera se puede apreciar eventos tanto de red como de host, los agentes, protocolos y un contador con el número de estos eventos. En las siguientes métricas se ve categorías de eventos y software encargado de recolectarlos con un contador:

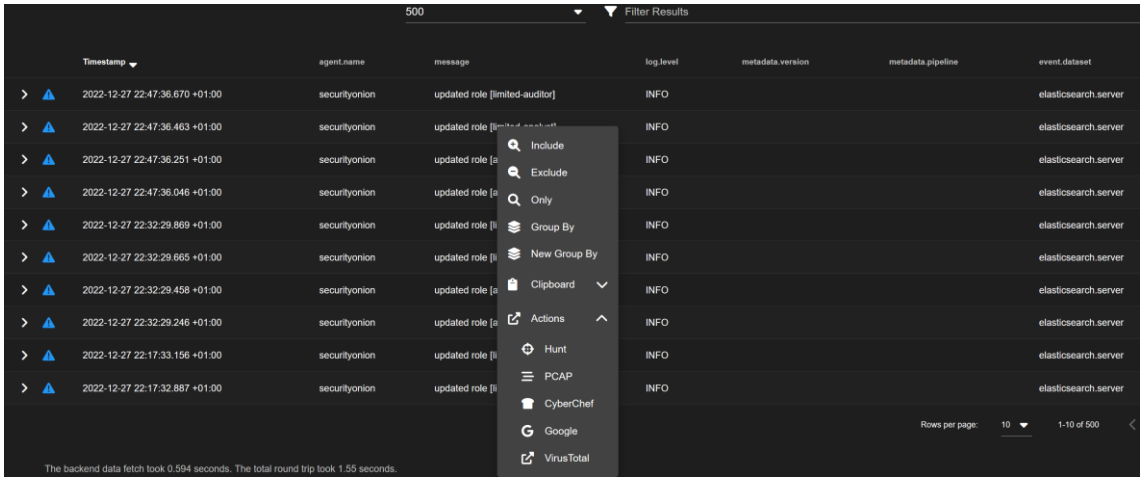




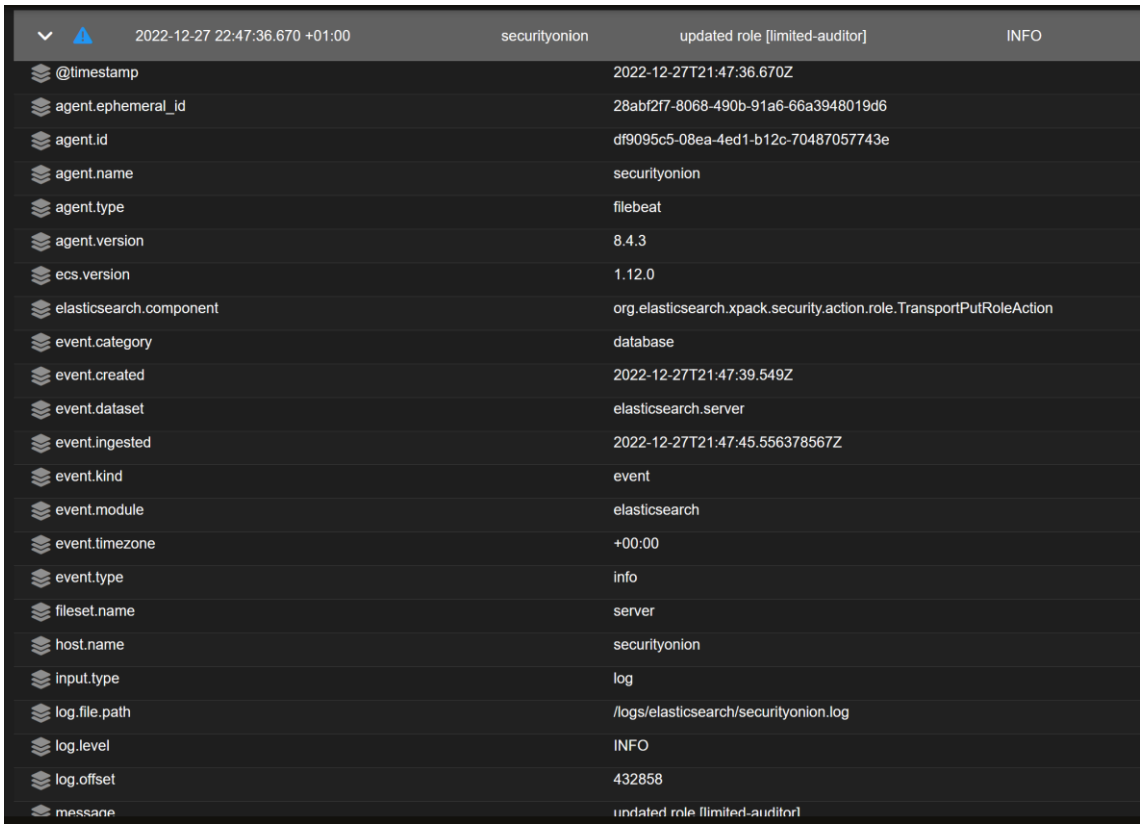
En la tercera parte de métricas se ven eventos agrupados por IP de destino y origen y puertos de destino:



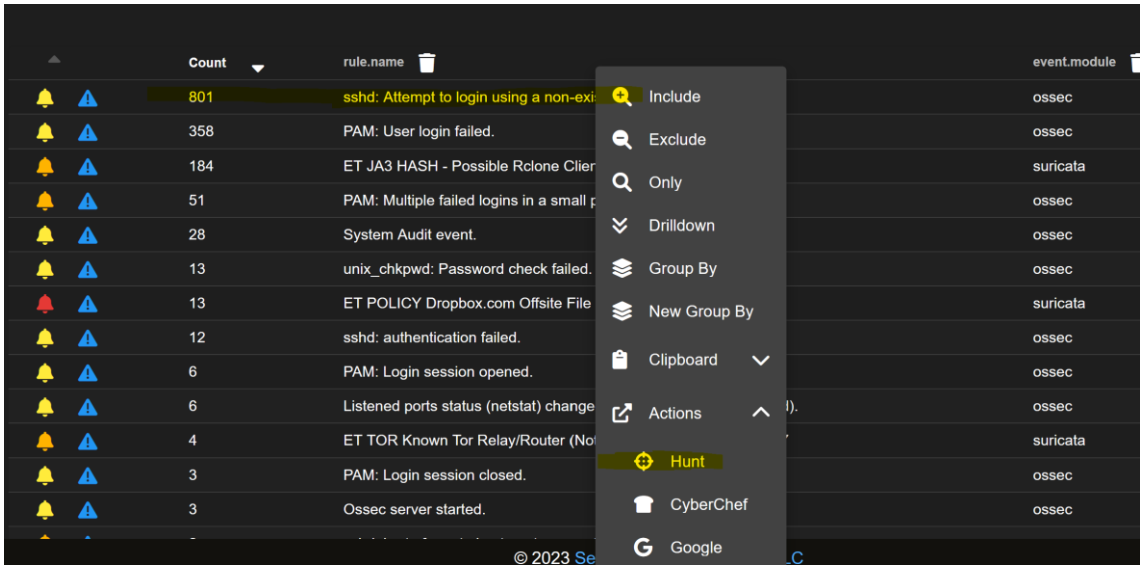
En la última métrica se ve una lista de los eventos, haciendo clic en el evento se puede ver las acciones que se puede tomar:



En la pestaña de la izquierda se despliega y se ve el log del evento:

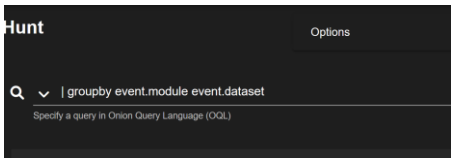


El apartado de Hunt está orientado a la caza compleja de amenazas o threat hunting y también para analizar exhaustivamente cualquier evento detectado por HIDS/NIDS. Para poner un ejemplo, en el panel de alertas al visualizar una alerta de red o de host clicando sobre el evento saldrá la opción de Hunt para un análisis:

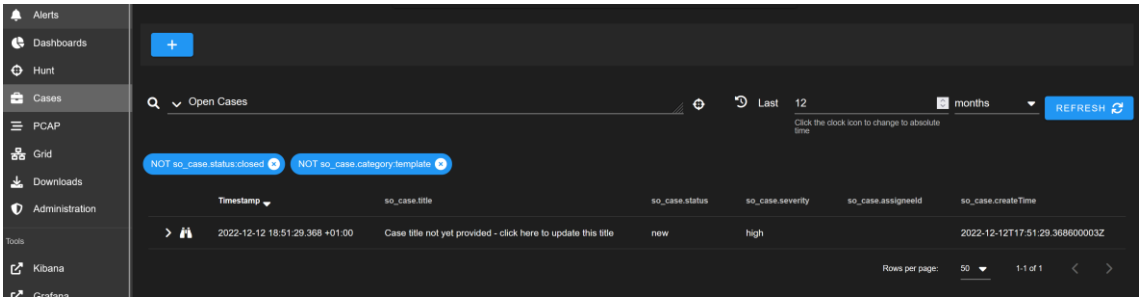


Se usará una herramienta para conectar a ssh probando múltiples credenciales, se examina con Hunt. Se abre el evento y se ve en log en formato Json, apreciando toda la información:

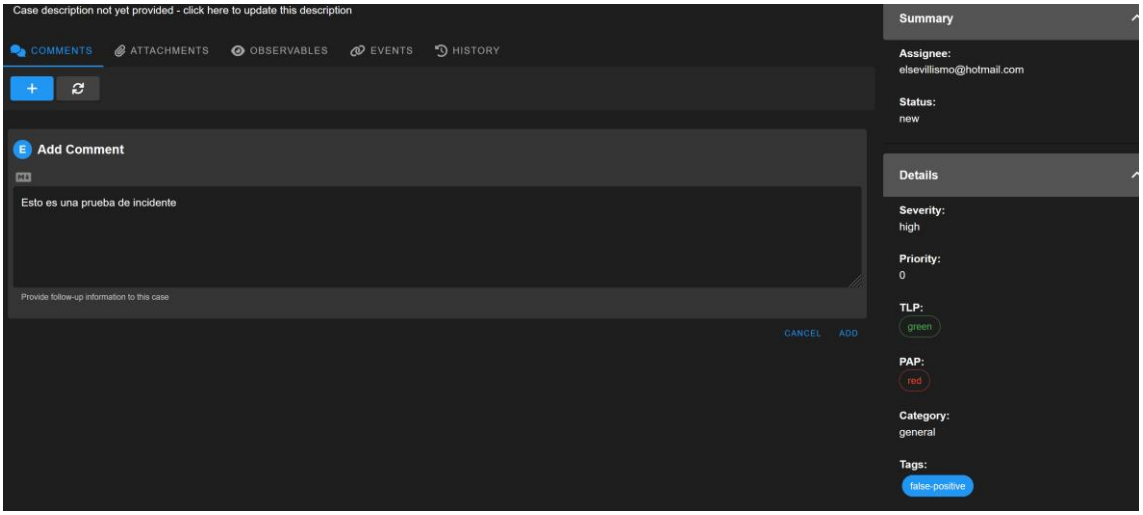
Se aprecia la Ip de origen, timestamp, name del evento, message…etc, toda la información que se necesita. En la búsqueda del apartado Hunt se aprecia que se debe de realizar en OQL (onion query language), está basado con la sintaxis Lucene.



El apartado Cases es la sección de ticketing similar a la que tiene OSSIM para cuando se vea un log o alerta sospechosa se puede crear directamente un caso o ticket.

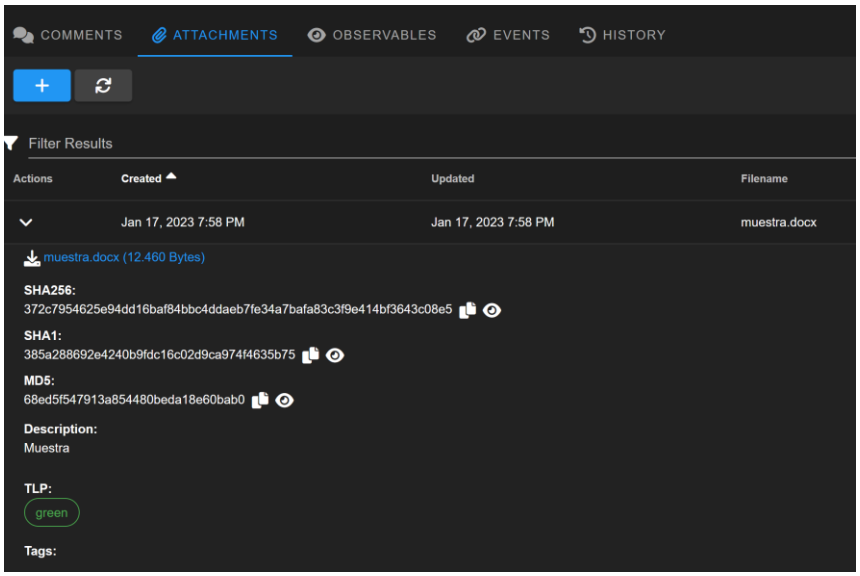


Para crear un nuevo caso se hace clic en el botón de + o también desde dashboards, Hunt o Alerts pinchando y elevando a cases:

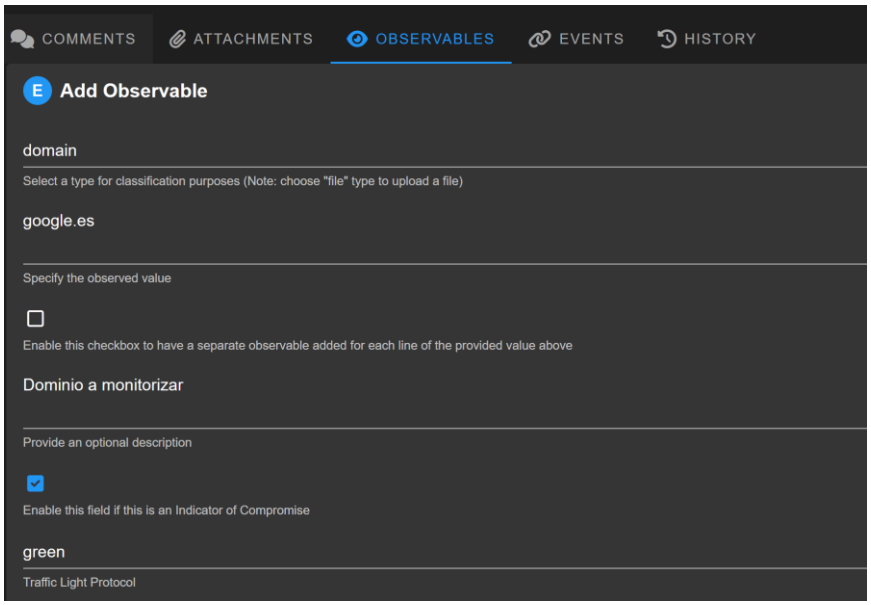


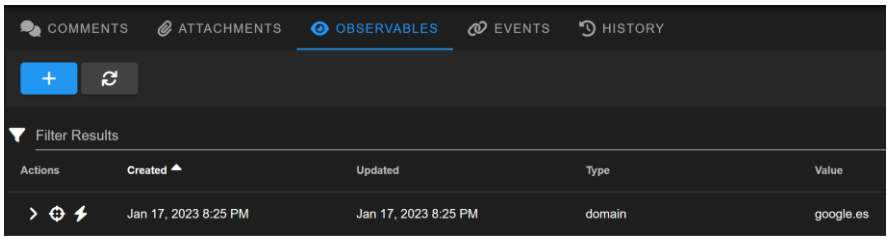
Hay muchas opciones para categorizar el incidente como el estado, severidad, prioridad, TLP (traffic light protocol) que es el nivel de clasificación de la información, PAP (Permissible Actions Protocol) similar al TLP indica como se debe de usar la información obtenida, categorías y por último etiqueta.

En adjuntos, se subirá los archivos que se considere y se definirá su TLP y aparte se calculará de forma automática el hash:



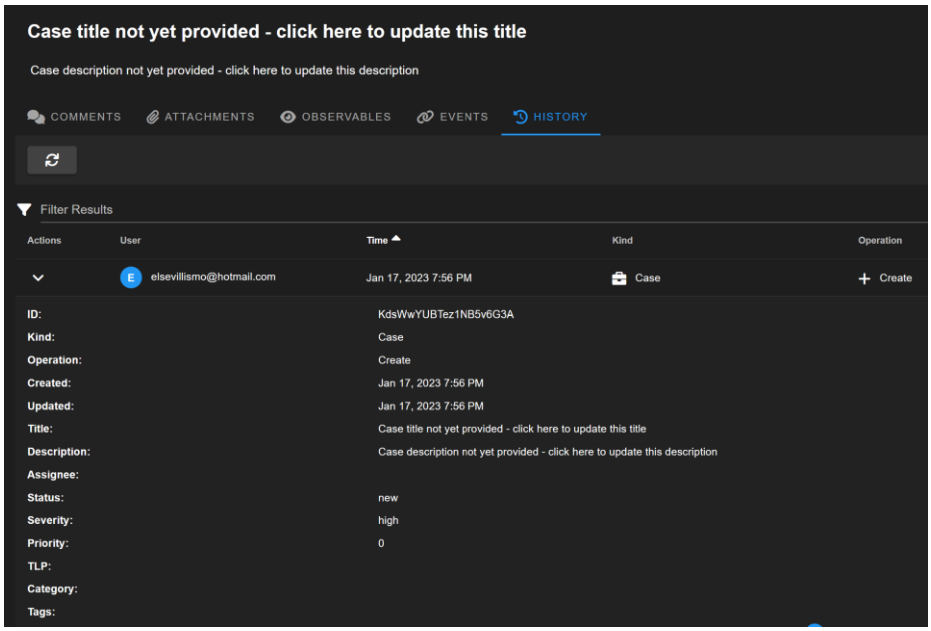
En el apartado de observable se puede añadir cualquier tipo de IOC para monitorizarlo:





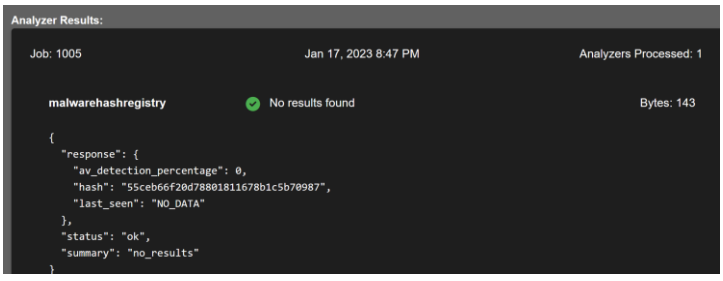
En el apartado de Events aparecen los casos escalados desde alertas de Suricata, ossec o zeek.

En el apartado de History aparece el historial del ticket, como cambios introducidos por otros usuarios, ampliación de adjuntos, IOC´s…etc.

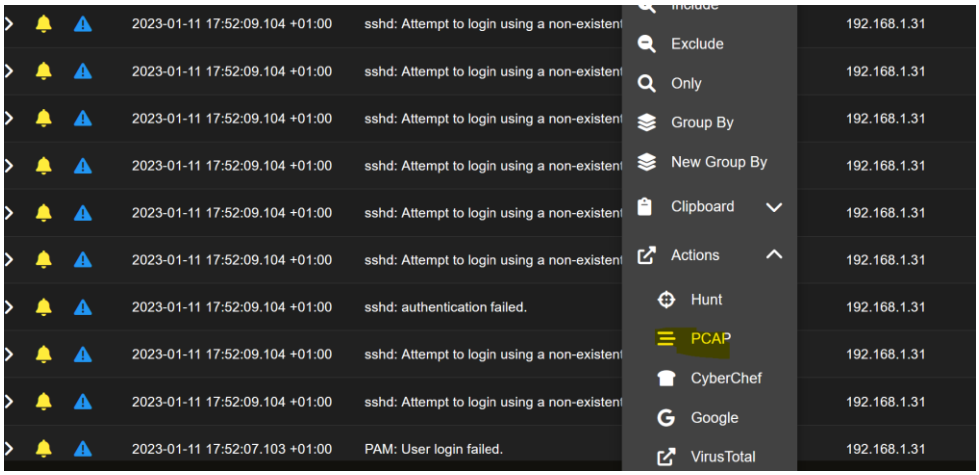


En observables donde se ha introducido un IOC que se puede analizar en diferentes fuentes de información en la que se esté registrado y previamente configurados en Onion:

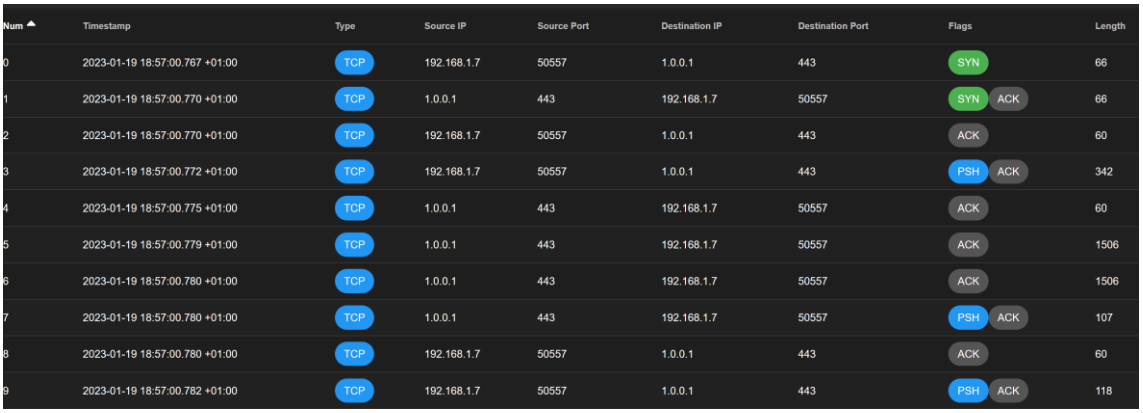
Name	Domain	Hash	IP	Mail	Other	URI	URL	User Agent
Alienvault OTX	✓	✓						✓
EmailRep				✓				
Greynoise			✓					
LocalFile	✓	✓	✓		✓		✓	
Malware Hash Registry		✓						
Pulsedive	✓	✓	✓			✓	✓	✓
Spamhaus			✓					
Urlhaus							✓	
Urlscan							✓	
Virustotal	✓	✓	✓				✓	
WhoisLookup	✓							



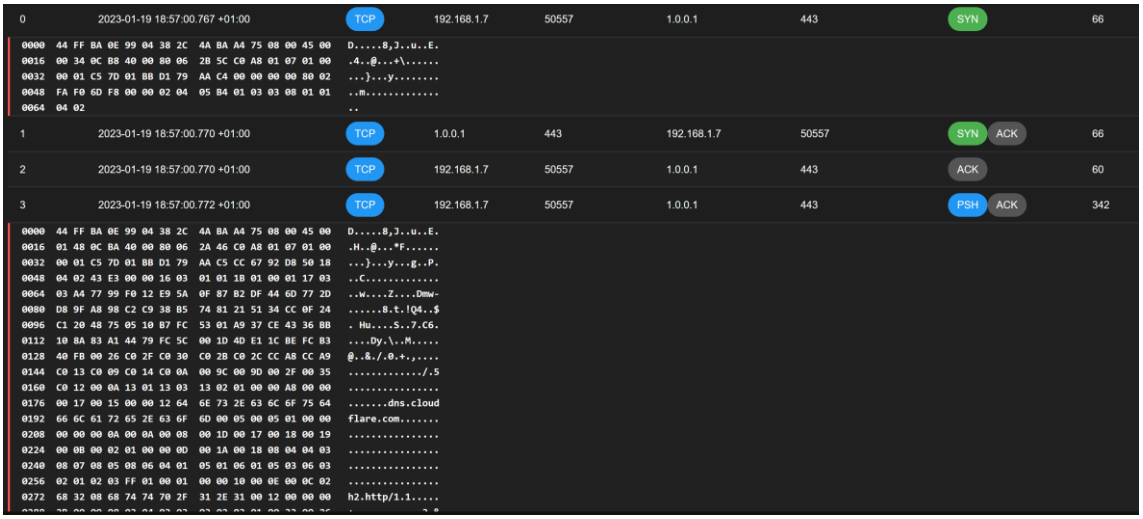
En el apartado PCAP, se puede analizar capturas de tráfico realizadas por Stenographer. El PCAP a analizar se obtendrá del panel de alertas, dashboards o Hunt:



Se elige el evento de sincronización con cliente cloud MEGA:

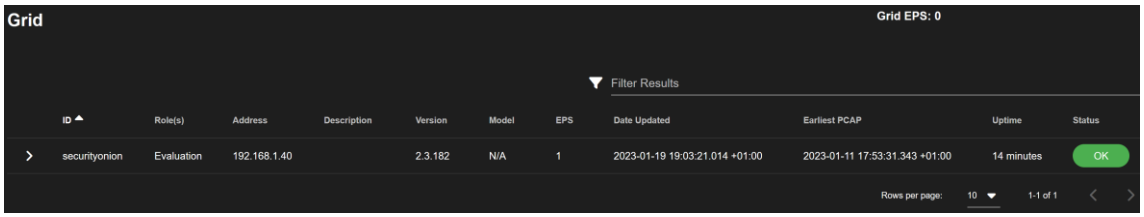


Num	Timestamp	Type	Source IP	Source Port	Destination IP	Destination Port	Flags	Length
0	2023-01-19 18:57:00.767 +01:00	TCP	192.168.1.7	50557	1.0.0.1	443	SYN	66
1	2023-01-19 18:57:00.770 +01:00	TCP	1.0.0.1	443	192.168.1.7	50557	SYN ACK	66
2	2023-01-19 18:57:00.770 +01:00	TCP	192.168.1.7	50557	1.0.0.1	443	ACK	60
3	2023-01-19 18:57:00.772 +01:00	TCP	192.168.1.7	50557	1.0.0.1	443	PSH ACK	342
4	2023-01-19 18:57:00.775 +01:00	TCP	1.0.0.1	443	192.168.1.7	50557	ACK	60
5	2023-01-19 18:57:00.779 +01:00	TCP	1.0.0.1	443	192.168.1.7	50557	ACK	1506
6	2023-01-19 18:57:00.780 +01:00	TCP	1.0.0.1	443	192.168.1.7	50557	ACK	1506
7	2023-01-19 18:57:00.780 +01:00	TCP	1.0.0.1	443	192.168.1.7	50557	PSH ACK	107
8	2023-01-19 18:57:00.780 +01:00	TCP	192.168.1.7	50557	1.0.0.1	443	ACK	60
9	2023-01-19 18:57:00.782 +01:00	TCP	192.168.1.7	50557	1.0.0.1	443	PSH ACK	118

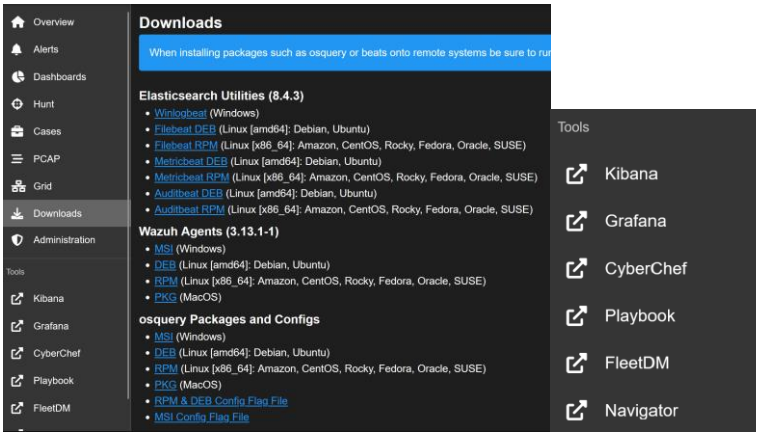


Se puede enviar a Cyberchef cuando se vea tráfico codificado y se puede descargar el archivo pcap para analizarlo con otra herramienta.

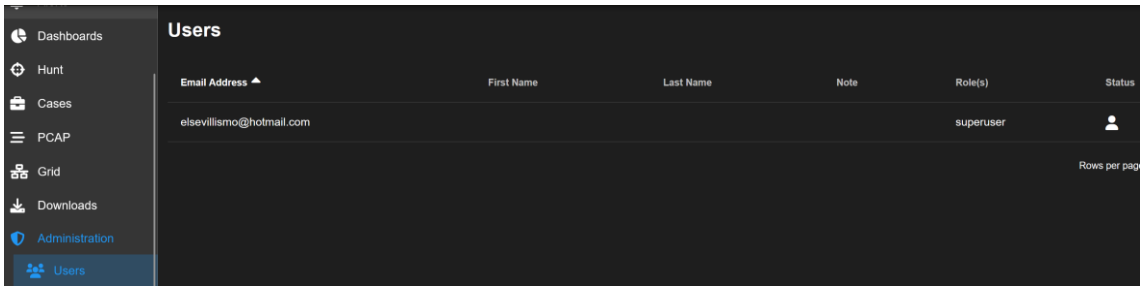
En el apartado de GRID se verá los sensores desplegados:



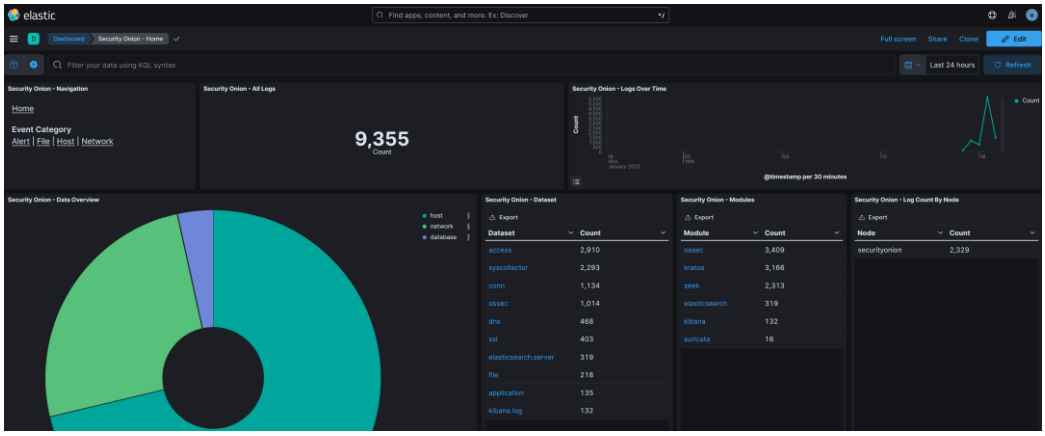
En la sección de descargas se encontrarán los agentes HIDS como ossec y wazuh y utilidades para elasticsearch:



Se tiene la parte de administración de usuarios:



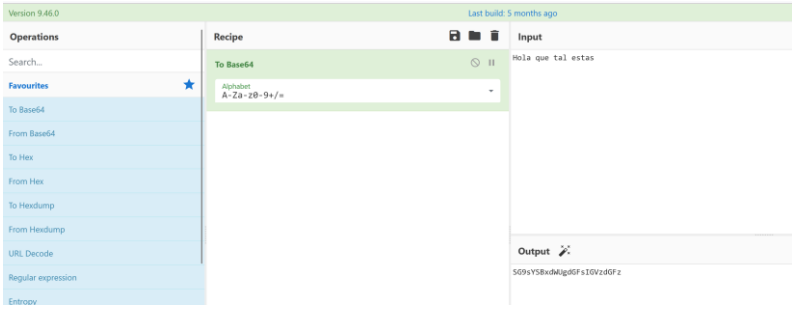
A continuación, está el acceso a Kibana, interfaz gráfica de Elastic:



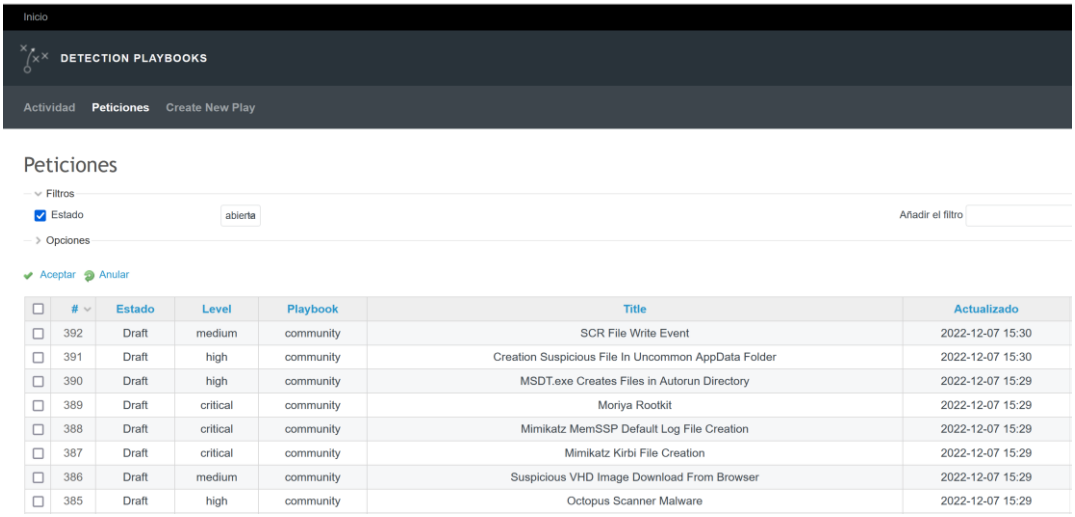
Elastic es el logger donde se realizan búsquedas para encontrar eventos.

Desde el panel principal de Onion está Grafana, donde da información de la salud del sistema, aparecen métricas de uso del hardware:

Se ve que se tiene la herramienta de cyberchef para análisis de artefactos:

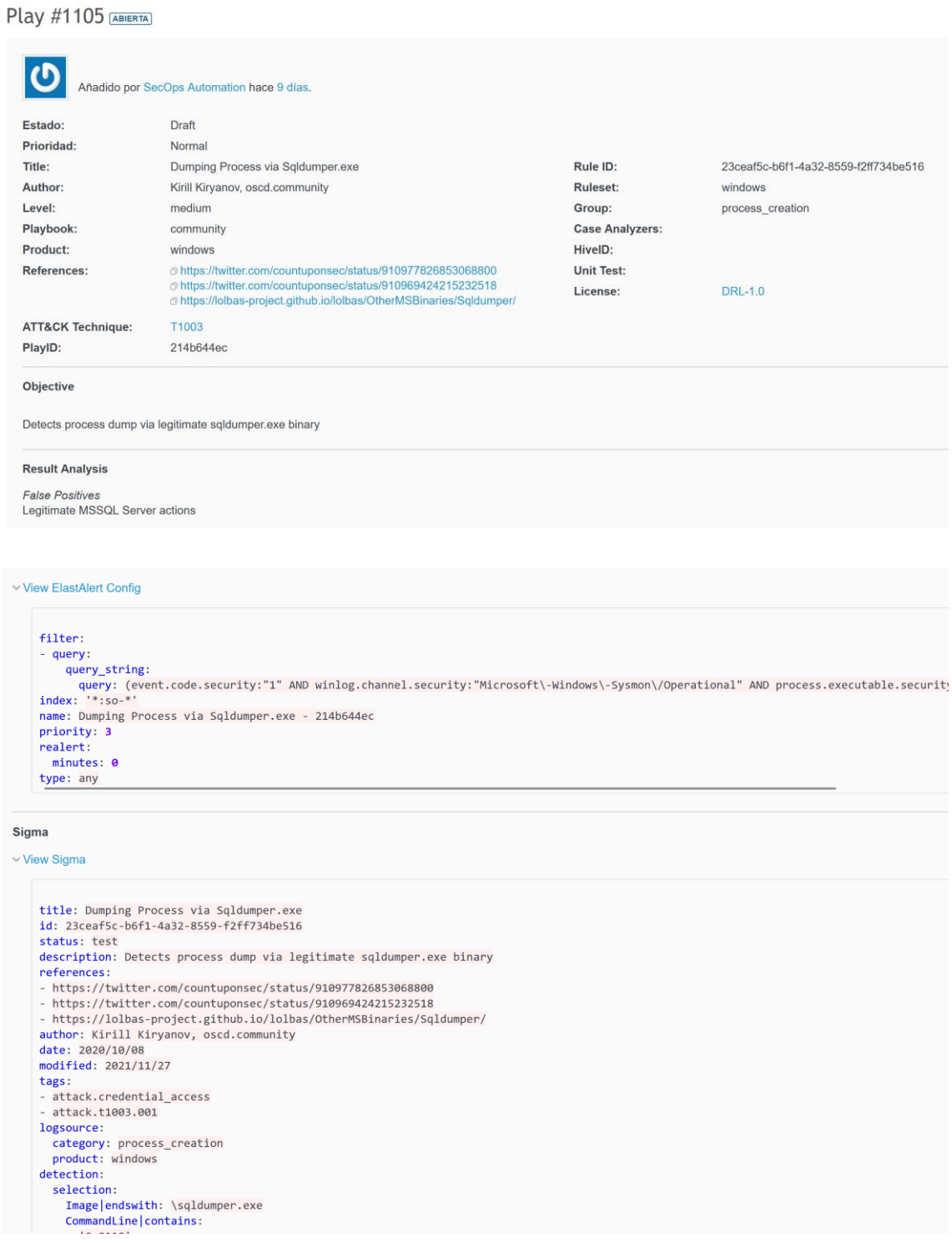


Otra herramienta más es la de playbook en la que se encuentran casos y estrategias para la detección y se podrá generar propias reglas:

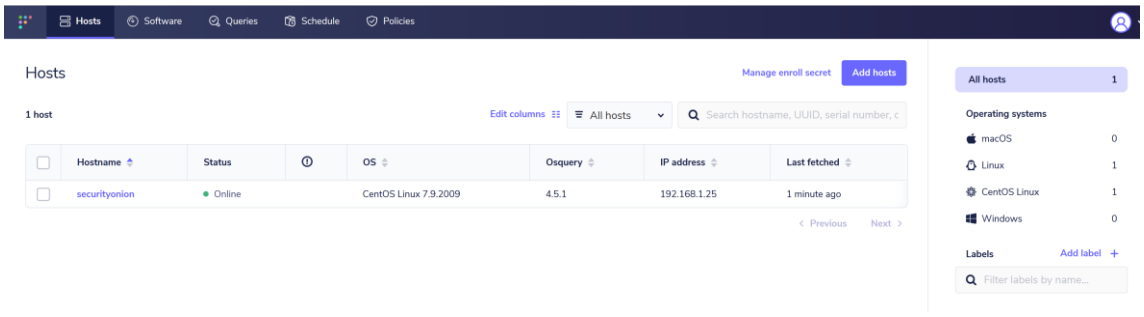


#	Estado	Level	Playbook	Title	Actualizado
392	Draft	medium	community	SCR File Write Event	2022-12-07 15:30
391	Draft	high	community	Creation Suspicious File In Uncommon AppData Folder	2022-12-07 15:30
390	Draft	high	community	MSDT.exe Creates Files in Autorun Directory	2022-12-07 15:29
389	Draft	critical	community	Moriya Rootkit	2022-12-07 15:29
388	Draft	critical	community	Mimikatz MemSSP Default Log File Creation	2022-12-07 15:29
387	Draft	critical	community	Mimikatz Kirbi File Creation	2022-12-07 15:29
386	Draft	medium	community	Suspicious VHD Image Download From Browser	2022-12-07 15:29
385	Draft	high	community	Octopus Scanner Malware	2022-12-07 15:29

Se puede editar o crear implementando reglas en Elastic y sigma:

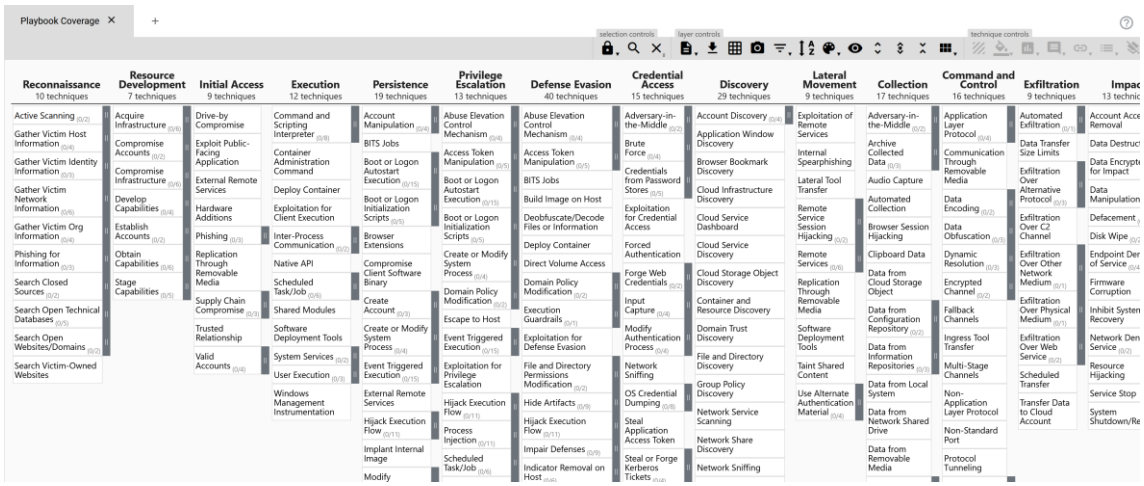


Otra herramienta es Fleetdm la que dará visibilidad y estado de los equipos, servidores, contenedores, en diferentes sistemas operativos desplegando osquery de la red instalando osquery:

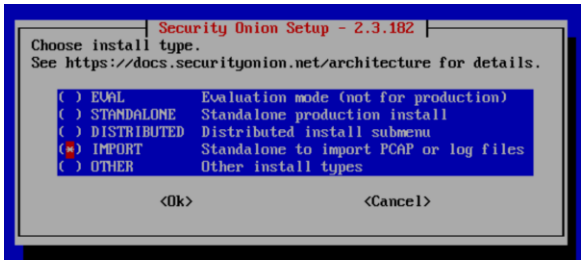


Se sabrá que usuarios han estado en los equipos, que hardware tiene cada equipo, que programas está instalados y que vulnerabilidades tienen y ver las GPO de la organización de cada usuario.

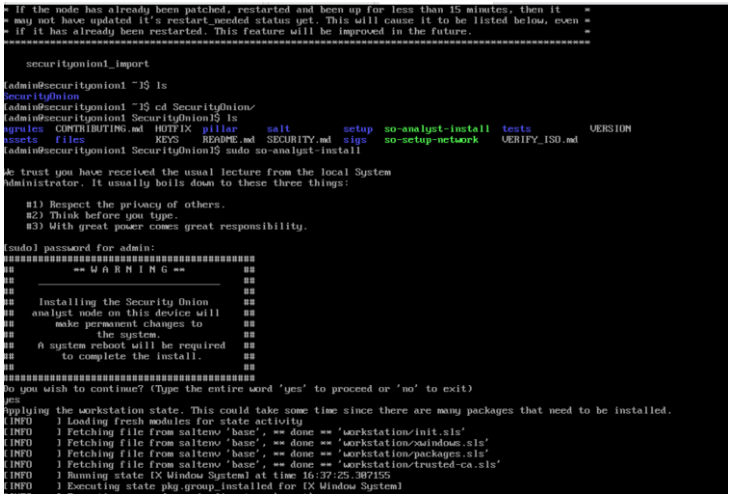
La herramienta de navigator permitirá visualizar el mapa de Mitre ATT&CK, se podrá editar la cobertura defensiva y la frecuencia de detección de técnicas y demás datos de los ataques detectados, se puede editar las celdas poner colores y demás.



Una vez visto todas las opciones se va a instalar la modalidad de IMPORT para analizar PCAP y realizar una prueba. Se realizará una instalación nueva siguiendo los pasos, pero ahora se elige el modo IMPORT:

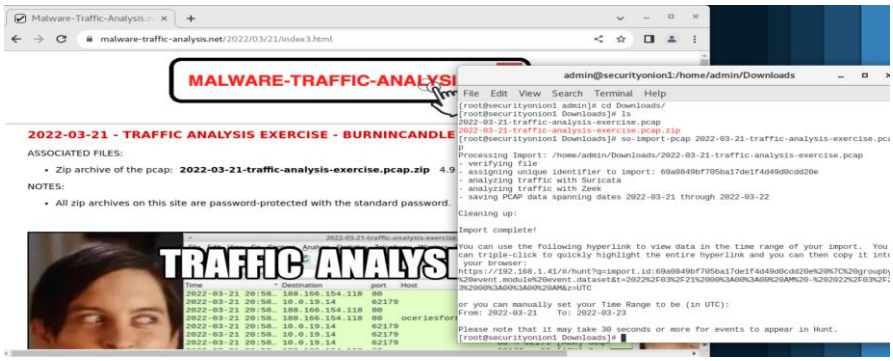


Se seguirán los pasos y al abrir la consola se tiene que instalar la consola de analista:



Finalizada la instalación se abre en modo de consola:

Una vez instalado se abre el navegador y se descarga un par de PCAP de prueba y se importa:



Al importarse los PCAP Suricata y ZEEK analizan los tráficos y sacan las siguientes alertas:

Count	rule.name	event.module
250	ET MALWARE Cobalt Strike Beacon Observed	suricata
216	ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)	suricata
142	ET JA3 Hash - [Abuse.ch] Possible Dridex	suricata
22	ET DNS Query to a *.top domain - Likely Hostile	suricata
10	ET MALWARE Tordal/Hancitor/Chanitor Checkin	suricata
5	ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1	suricata
3	GPL NETBIOS SMB IPC$ unicode share access	suricata
2	ET POLICY DNS Update From External net	suricata
2	ET PHISHING Lets Encrypt Free SSL Cert Observed with IDN/Punycode Domain - Possible Phishing	suricata
2	ET MALWARE Win32/Ficker Stealer Activity M3	suricata
2	ET MALWARE Win32/Ficker Stealer Activity	suricata
1	ET POLICY PE EXE or DLL Windows file download HTTP	suricata
1	ET POLICY External IP Lookup api.ipify.org	suricata
1	ET POLICY External IP Lookup (ipify .org)	suricata
1	ET MALWARE Win32/IcedID Request Cookie	suricata
1	ET MALWARE Meterpreter or Other Reverse Shell SSL Cert	suricata
1	ET INFO Packed Executable Download	suricata
1	ET INFO HTTP Request to a *.top domain	suricata
1	ET HUNTING Suspicious Empty SSL Certificate - Observed in Cobalt Strike	suricata

Se va a proceder a explicar las reglas más importantes detectado en los PCAP que detecta Suricata:

ET JA3 Hash - [Abuse.ch] Possible Dridex.

Alerta de una posible ejecución en la red del malware Dridex. Dridex en un primer lugar de distribuye en correos maliciosos con un Word o Excel con macros adjunto y en cuanto se ejecuta conecta con su servidor C2 para avanzar en diferentes fases. Su finalidad es obtener credenciales bancarias rastreando los dispositivos.

ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1.

Esta alerta informa de que se están realizando peticiones POST de un user-agent que corresponde con navegadores falsos. Es muy probable que estas peticiones se realicen desde la red por bots ya sea para intenciones maliciosas como denegaciones de servicio.

ET MALWARE Win32/Ficker Stealer Activity.

La alerta Ficker Stealer Activiy informa que hay actividad en la red del malware Ficker. El malware Ficker lo que hace es crear aplicaciones maliciosas que parecen visualmente legítimas en páginas web falsas. Si se accede a esas webs y se ejecutan esas aplicaciones los atacantes tienen la posibilidad de robar datos en el sistema.

ET PHISHING Lets Encrypt Free SSL Cert Observed with IDN/Punycode Domain - Possible Phishing.

La organización Lets Encrypt proporcionar certificados bajo pago con los que proporcionan seguridad en las páginas web. Sin embargos hay certificados de Lets Encrypt que han sido modificados para dominios que contienen Punycode, es decir, con Punycode los nombres de la web falsa que contienen caracteres Unicode se codifican en un subconjunto de ASCII que consta de letras, dígitos y guiones, que se denomina subconjunto de letras, dígitos y guiones intentando emular a la legítima.

ET MALWARE Cobalt Strike Beacon Observed.

Esta alerta detecta un beacon o señal ya sea de navegación o contacto por IP de contacto al dominio Cobal Strike. En este dominio se encuentran multitud de herramientas para penetración en sistemas y redes.

ET MALWARE Tordal/Hancitor/Chanitor Checkin.

Detectada alerta de posible ejecución de malware del tipo troyano. El atacante obtuvo acceso inicial a un sistema a través de una campaña que hizo uso del downloader Hancitor. La DLL de la primera etapa, que fue eliminada por un documento de Word malicioso, intentó descargar varias cargas útiles de malware en el host, incluido Ficker Stealer. Además, se descargó e implementó una carga útil de Cobalt Strike para actividades posteriores a la explotación.

ET HUNTING Suspicious Empty SSL Certificate - Observed in Cobalt Strike.

Alerta de dominios con certificados no completos, suelen ser certificados de nivel de dominio que se venden por ciertas autoridades como Lets Encrypt por módicos precios. Aunque se vean dominios con seguridad SSL/Https hay que fijarse en el tipo de certificado que tienen y ver sus características.

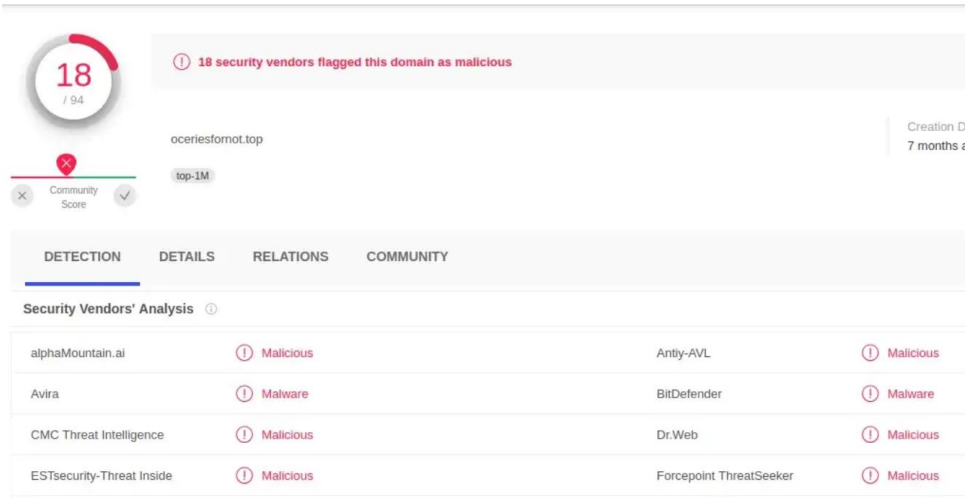
ET MALWARE Meterpreter or Other Reverse Shell SSL.

Informa que ha detectado uso de meterpreter o una reverse shell cifrada. Meterpreter es el payload creado con la herramienta Metasploit para mantener comunicaciones con el host víctima y realizar tareas de forma remota. Detecta el payload y lo asocia con una consola cifrada en remoto.

ET MALWARE Win32/IcedID Request Cookie.

Esta alerta informa de que probablemente este infectados con el malware IceID. Esta alerta está conjuntamente relacionada con "ET INFO HTTP Request to a *.top domain", ya que el dominio C2 es *.top. Esto se confirma con la cookie ya que se ve que el host al que va la petición GET HTTP:

Con lo cual al ver este dominio se comprueba en virustotal que es malicioso:



ET POLICY External IP Lookup (ipify .org).

Alerta de que están realizando un lookup a una IP, osease sacar información de la IP a través de API de ipify.org. Puede ser parte de un malware que extrae geolocalización de la IP y según el país continúa atacando o se para. Es muy común verlo en ransomware, extrae información de la IP y si no es de un país ruso, o de la antigua unión soviética continua el ataque.

ET POLICY PE EXE or DLL Windows file download HTTP.

Esta alerta informa que se ha descargado desde http un ejecutable para Windows o un archivo con extensión dll. Por lo general suele ser falsos positivos, a menos que en las políticas de seguridad (GPO) se haya denegado este tipo de descargas. Lo que se puede hacer es realizar un análisis al archivo manual y mediante sandbox para confirmar que es legítimo y no un malware.

4.4 Organización del capítulo.

En este capítulo se ha visto el despliegue la plataforma de despliegue de incidentes y de los dos SIEM.

Primeramente, se siguen las guías CCN-STIC para la instalación y configuración de LUCIA.

Se define el ciclo de vida de un incidente en LUCIA, se define los términos de investigación, reporte de incidente, así como también el ciclo de vida de un ticket creado con un ejemplo de flujo de trabajo.

A continuación, se describe el proceso de instalación del SIEM secundario o de back-up AlienVault. Se despliega el agente de host ossec y se comprueba su correcto funcionamiento. Se describen los menús, dashboards y configuración.

Por último, se describirán los programas del que está formado. Se definirá sus diferentes arquitecturas, la que se va a desplegar y testear. Se probará dos arquitecturas, en la principal y modo evaluación se definen todos los dashboards que trae la solución Security Onion.

Se instala también otra arquitectura para análisis de PCAP, simulando ataques y se comprueba como el SIEM detecta y clasifica estos tipos de ataques.

5. Conclusiones.

A continuación, se presenta una visión global del trabajo realizado, las ventajas y desventajas que presenta trabajar implementar un SOC con un SIEM. También se establece una conclusión final para verificar el objetivo y se abordan futuras líneas de investigación.

5.1 Visión global del trabajo y verificación de objetivos.

Se ha realizado una solución empresarial atendiendo a la nueva ley de las start-up, para la creación del tipo de SOC que se desee, el cual monitorizará el tráfico de la red y de los host notificando los eventos de seguridad.

El SIEM es una pieza muy importante en un centro de operación de seguridad (SOC), pero no sólo se puede confiar en los aspectos técnicos del SIEM. El tiempo utilizado para el desarrollo de la configuración de un SIEM, es necesario para minimizar esfuerzo en pasos futuros. La parte más grande de la configuración merece especial atención, y es importante recordar que la base de la infraestructura son las fuentes de eventos, es decir los dispositivos y no el sistema SIEM. Es una herramienta compleja que recolecta, almacena, normaliza, correlaciona y analiza información de datos de un gran número de dispositivos de red con los cuales es capaz de entregar inteligencia de seguridad, además de una referencia sobre el comportamiento típico de una red.

Se concluye que se ha cumplido el objetivo de poder testear herramientas esenciales y principales para constituir un SOC viendo que ha sido posible su despliegue y correcto funcionamiento.

Se ha analizado el mercado de los contratos de licitación públicos, se analizan los requisitos del Esquema Nacional de Seguridad y los requisitos que solicitan para cumplir la normativa, formar parte de la red nacional de SOC, concluyendo que se puede acercarse a casi todos con suficiente experiencia, personal y material.

5.2 Ventajas e inconvenientes de la solución desarrollada.

Se ha analizado los objetivos de un SOC y de su motor principal, el SIEM. También se ha analizado las funcionalidades principales y las propias del sistema elegido en este proyecto teniendo todas las herramientas open-source.

Sin embargo, a pesar de todas las ventajas que presenta, también aparece uno de los principales inconvenientes de las herramientas SIEM, el cual consiste en analizar las causas de cualquier evento que amenace la seguridad puede tardar un tiempo considerable, lo que puede ocasionar que las respuestas ante tal evento puedan ser en algunos casos tardías.

Se concluye con dos inconvenientes, uno de ellos sería albergar la solución SOC en la nube y depender de servicios de terceros, posibles caídas de servicio, latencia, brechas de seguridad, protección de datos a un externo…etc. Aunque ahorraría gran costo económico en hardware en caso de que el organismo no lo proporcione, que lo normal es que si lo proporcione, se dependería de servicios de terceros.

Al igual que es una ventaja económica la solución open-source, el gran inconveniente es el soporte. Al no tener un soporte personalizado cualquier problema del sistema se tiene que solventar por uno mismo. Siempre se puede atender al foro y presentar dudas, pero tarda en resolverse y no es siempre muy preciso.

5.3 Trabajos futuros y líneas de investigación propuestas.

Como medidas de mejoras en un futuro para el SIEM sería desplegarlo en su versión distribuida con un mayor número de sensores, search y manager e instalar diferentes agentes (wazuh, osquery) en todos los host y comparar los eventos recibidos. A su vez, sería interesante probar un despliegue en cloud ya sea con AWS o Azure.

Sería interesante la integración con aplicaciones de IA y de machine learning, así como implementar proxy de navegación, antivirus para servidor de correo y firewall del tipo software como pfsense para ir realizando más pruebas de integración.

6. Glosario de términos.

- API (Aplication Programming Interface): protocolo de comunicación o interfaz entre diferentes partes de un software.
- APT (Advanced Persistent Threat): ataque dónde se gana acceso a un computador o red por un periodo de tiempo extenso sin ser detectado.
- CPD (Centro de Procesamiento de Datos): espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización
- DNS (Domain Name System): sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.
- GPO (Group Policy Object): conjunto de reglas que controlan el entorno de trabajo de cuentas de usuario y cuentas de equipo.
- IDS (Intrusion Detection System): programa de detección de accesos no autorizados a un computador o a una red.
- IPS (Intrusion Prevention System): programa de prevención de accesos no autorizados a un computador o a una red.
- CERT/CSIRT (Computer Emergency Response Team/Computer Security Incident Response Team). Equipo de respuesta (o preparación) para emergencias informáticas / Equipo de Respuesta a Incidentes de Seguridad.
- REST (Representational State Transfer). Arquitectura de software para realizar una comunicación cliente-servidor
- SIEM (Security Information And Event Management). Sistema de gestión de información y eventos de seguridad.
- SOC **(**Security Operation Center). Centro de seguridad informática.
- CISO (Chief Information Security Officer). Responsable de velar por la ciberseguridad de una empresa
- EDR (Endpoint Detection and Response). Herramienta que proporciona monitorización y análisis continuo del endpoint.
- SOAR (Security Orchestration, Automation and Response). Orquestación, automatización y respuesta de seguridad

- DMZ (demilitarized zone). Zona desmilitarizada.
- DDoS (Distributed Denial of Service). Denegación de servicio distribuido.
- NIST (National Institute of Standards and Technology). El Instituto Nacional de Estándares y Tecnología.
- CEO (Chief Executive Officer). Director general o consejero delegado.
- ISO (Internacional Organization for Standardization). Organización Internacional de Normalización.
- CCN. Centro criptológico nacional.
- RFC (Request for Comments). Publicaciones del grupo de trabajo de ingeniería.
- IETF (Internet Engineering Task Force). Grupo de Trabajo de Ingeniería de Internet.
- OTX (Open Threat Exchange). Intercambio Abierto de Amenazas de AlienVault.
- RT/RTIR (Request Tracker Incident Response). Sistema de gestión de incidentes.
- MISP (Malware Intelligence Sharing Platform). Plataforma de compaertición de amenazas.
- IOC (Indicator of compromise). Indicador de compromiso.
- OSINT (Open Source Intelligence). Inteligencia de fuentes abiertas.
- OSSIM (Open Source Security Information Management). Herramientas open source de seguridad de la información.
- USM (Unified Security Management). Gestión de Seguridad Unificada.
- SAT. Sistema de alerta temprana.
- SPAM (Shoulder of Pork Ham). Mensajes de correo electrónico no solicitados.
- NAT (Network Address Translation). Traducción de dirección de red.
- ROI (Return On Investment). Retorno de la inversión.

7. Bibliografía.

[1] Instituto Nacional de Ciberseguridad: www.incibe.es

[2] SOC as a Service: qué es y por qué mejora la seguridad. https://www.redeszone.net

[3] Como construir un Centro de Operaciones de Seguridad (SOC) efectivo en tu empresa. https://ayudaleyprotecciondatos.es

[4] ¿Qué es un centro de operaciones de seguridad (SOC)? https://ciberseguridad.com/

[5] ¿Crear un SOC desde cero o contratar uno externo? https://www.sofistic.com

[6] Comparación entre el SOC como servicio y la plataforma SOC basada en la nube. https://www.cyrebro.io

[7] Computer Security Incident Handling Guide. https://csrc.nist.gov

[8] El CCN pone en marcha la Red Nacional de Centros de Operaciones de Ciberseguridad. https://administracionelectronica.gob.es/

[9] Red nacional de SOC. https://rns.ccn-cert.cni.es/

[10] The EU's Cybersecurity Strategy for the Digital Decade https://digital-strategy.ec.europa.eu

[11] CCN https://www.ccn.cni.es/

[12] IT Digital Security https://www.itdigitalsecurity.es/

[13] Ministerio de asuntos económicos. https://portal.mineco.gob.es

[14] Sociedad limitada, ventajas y características. https://www.infoautonomos.com

ANEXO

OBJETIVOS DE DESARROLLO SOSTENIBLE

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	Alto	Medio	Bajo	No Procede
ODS 1. **Fin de la pobreza.**				X
ODS 2. **Hambre cero.**				X
ODS 3. **Salud y bienestar.**				SI
ODS 4. **Educación de calidad.**				X
ODS 5. **Igualdad de género.**				SI
ODS 6. **Agua limpia y saneamiento.**				SI
ODS 7. **Energía asequible y no contaminante.**				SI
ODS 8. **Trabajo decente y crecimiento económico.**				SI
ODS 9. **Industria, innovación e infraestructuras.**				SI
ODS 10. **Reducción de las desigualdades**.				X
ODS 11. **Ciudades y comunidades sostenibles**.				X
ODS 12. **Producción y consumo responsables.**				SI
ODS 13. **Acción por el clima.**				X
ODS 14. **Vida submarina.**				X
ODS 15. **Vida de ecosistemas terrestres.**				X
ODS 16. **Paz, justicia e instituciones sólidas.**				SI
ODS 17. **Alianzas para lograr objetivos.**				SI

Reflexión sobre la relación del TFM con los ODS.

Este trabajo está relacionado al 30% con los objetivos de desarrollo sostenible. A continuación, se va a definir cada uno y explicar la relación con el ODS:

ODS 3. Salud y bienestar: Es importante hoy en día la conectividad entre la medicina y el paciente. Estos últimos años se ha comprobado con el COVID-19 el aumento que hubo de ataques al sector sanitario. De hecho, se produjo la primera muerte por un ataque informático en un hospital de Alemania. Se ha visto como los SOC crecieron exponencialmente no solo en el sector sanitario sino en el de vacunas, hospitales…etc.

ODS 5. Igualdad de género: En el proyecto se habla de la importancia de captar un contrato público, el cual por el sistema de puntuación obliga a contratar personal para atender el SOC fuera de horario laboral. En este momento en el que se contratan nuevos empleados se debe basarse e implementar la igualdad de género. Se quiere decir que, a la hora de examinar los curriculum no se hará ninguna distinción entre género. Solo se atenderá la experiencia y formación para evaluar y contratar la persona que se crea más idónea para el puesto sin incidir en el género.

ODS 6. Agua limpia y saneamiento: Durante la realización de este Master se vió un caso de un ataque informático a una planta de depuración de agua en los Estados Unidos de América. Lo cual se extrapola este trabajo a la creación de un SOC para este tipo de infraestructuras. Un ataque de este tipo tiene consecuencias extremas en una población, pudiendo dejar sin agua potable por unos días a la población.

ODS 7. Energía limpia y asequible: Cada vez las personas y empresas disponen de muchos dispositivos electrónicos los cuales necesitan energía eléctrica para funcionar. Esta energía en un futuro cercano debería ser proveniente de una fuente de energía verde. En este proyecto se habla de poder usar electrónica online con servicios por internet el cual se reducirá el consumo energético y permitirá ahorrar en la compra de más dispositivos hardware. Todo esto incide en un ahorro de consumo eléctrico. Aparte de lo comentado, en las centrales nucleares para fabricar energía eléctrica es más que necesario la existencia de un SOC para evitar un desastre natural a gran escala en el planeta.

ODS 8. Trabajo decente y crecimiento económico: Uno de los objetivos de este trabajo es crecer laboralmente, dar un paso más allá e intentar crecer tanto económicamente como profesionalmente. Se pretende que con un cierto grado de experiencia y una alta cualificación

profesional, un grupo de compañeros pueda crear una nueva empresa para ofrecer servicios de ciberseguridad que hoy en día están tan demandados.

ODS 9. Industria, innovación e infraestructuras: Como se ha comentado anteriormente en infraestructuras críticas e industria es obligatorio disponer de un SOC, ya que los efectos de un ataque informático son catastróficos a nivel económico y social. Por poner un ejemplo, en Estados Unidos en el mes de enero de 2023 se produjo un error informático, supuestamente causado por un ataque, en el sistema aeroportuario el cual causó miles de retrasos y cancelaciones. Supone unas pérdidas económicas y una frustración y ansiedad en su sociedad.

ODS 12. Producción y consumo responsables: Se menciona ahora el problema mundial de residuos de aparatos electrónicos con su correspondiente consumo energético. En el trabajo se expone la posibilidad de operar hardware online con el consiguiente ahorro de hardware, el cual en un futuro cercano se convertirá en residuo electrónico.

ODS 16. Paz, justicia e instituciones sólidas: Los servicios electrónicos que brindan un organismo público al ciudadano son importantes. En este trabajo se considera implantar un SOC para la monitorización en un ayuntamiento local, lo cual velaría por la seguridad de los datos personales de la sociedad con el organismo público.

ODS 17**.** Alianzas para lograr objetivos: En el trabajo comentando la red nacional de SOC se ha explicado la relación y colaboración entre el sector público y privado. Se necesita afianzar alianzas entre estos sectores en cuestión de ciberseguridad luchando juntos contra las ciber amenazas en forma de compartir información y demás recursos.