Universitat Oberta de Catalunya

uoc.edu

Implementación de las operaciones y la gestión de un SOC en una institución financiera partiendo desde cero utilizando soluciones SIEM

Daniel Rodriguez Fueyo
Grado en Tecnologías y Servicios de Telecomunicación
Administración de redes y sistemas operativos

Miguel Martín Mateo
Javier Panadero Martínez

7 de junio de 2020

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Implementación de las operaciones y la gestión de un SOC en una institución financiera partiendo desde cero utilizando soluciones SIEM*
Nombre del autor:	*Daniel Rodríguez Fueyo*
Nombre del consultor/a:	*Miguel Martín Mateo*
Nombre del PRA:	*Javier Panadero Martínez*
Fecha de entrega (mm/aaaa):	06/2020
Titulación:	*Grado en Tecnologías y Servicios de Telecomunicación*
Área del Trabajo Final:	*Administración de redes y sistemas operativos*
Idioma del trabajo:	*Español*
Palabras clave	*Ciberseguridad, SIEM, SOC.*

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

La finalidad para realizar este proyecto es la muestra desde principio a fin de la implementación de un centro de monitorización de amenazas de ciberseguridad (SOC), un tema muy de actualidad y con mucho potencial hoy en día. Este centro basará su monitorización en soluciones SIEM a nivel profesional.

La metodología aplicada se basa en dos pilares, se implementarán por un lado las operaciones del centro (implementaciones, monitorización, configuración) y, por otro lado, todos los aspectos relacionados con la gestión, estos últimos realizados principalmente por la dirección del centro.

El contexto empleado se centra en la aplicación de un SOC para una gran empresa, en este caso del sector financiero. Se debe implementar un SOC funcional en un periodo relativamente corto debido a requerimientos por parte de las entidades supervisoras a nivel nacional y europeo, ya que es una de las condiciones mínimas exigidas para poder operar con la licencia proporcionada por este organismo.

Al finalizar el proyecto, se ha podido proporcionar al cliente (compañía Fincomp) con la implementación de dos soluciones SIEM (Qradar y Splunk), junto con los procedimientos para la gestión de los diferentes aspectos del día a día, como procedimiento de respuesta ante desastres, creación de casos de uso o entrenamiento de nuevos analistas. Todo ello sin desviarse demasiado del presupuesto inicial.

Uno de los aspectos en los que no se ha profundizado al máximo ha sido en el empleo de las características de Splunk, centrándose más en Qradar como SIEM principal.

Abstract (in English, 250 words or less):

The concept of the Security Operation Center division became very popular method of cyber-risk mitigation at the beginning of the 2010s, the main task of these kind of divisions is to monitor the security threats that companies could face in their day-to-day operations. With the implementation of a SOC, the possible cybersecurity threats can be detected and mitigated in a reasonable time manner.

The objective of this project is to provide the implementation of the SOC operations and Governance starting from the technical point of the SIEM solutions, and continuing with the creation of the processes and procedures needed to maintain the daily operations, including as well posible Audit excercise from internal/external partners.

The goal of this proposal is to be able to start the operations phase and prepare all the technical documents and processes which can facilitate that the organization starts the monitoring of the network activity based on them, respond and have the tools fully operational.

As there is no access to the huge resources needed in this case to create a full implementation, the proposed project will attempt to replicate in a small environment all the steps that should be done on a big scale network to face a real threat and try to mitigate the impact.

In order to create a good view on how a SOC is working, the student will assume the role of a Security Operations Center Manager, like this, the project will acquire a better visibility from the operations and governance perspective.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

1.1.1 Ámbito de aplicación del proyecto

El ámbito para aplicar este proyecto englobaría cualquier organización dispuesta a aplicar la implementación de un SOC en sus instalaciones. Para este proyecto en concreto, se van a incluir reglas a monitorizar y casos de uso que se extienden mayormente a las compañías financieras (sistemas de pago, infraestructura específica), por lo que se debería considerar la opción de eliminar estos pequeños ajustes para hacer la implementación más general.

Las variaciones entre compañía y compañía dependerán mayormente del presupuesto de esta, y el número de elementos a monitorizar de los que disponga (número de servidores, endpoints, impresoras, usuarios).

La utilización de algunas de las herramientas SIEM utilizadas tienen un coste económico bastante alto; en este caso se ha optado por una solución mixta entre Qradar y Splunk, los cuales llevan unas licencias de soporte de precio elevado (se incluirán costes más adelante en la memoria), pero siempre se puede optar por SIEMs más baratos o incluso soluciones basadas en Open Source (Elastic, por ejemplo). Debido a esto, muchas pequeñas y medianas empresas optan por externalizar los servicios a otros SOC por un precio bastante inferior. En el caso de este proyecto hablamos de un SOC interno al 100%.

En la realización de este proyecto se ha utilizado como ejemplo una empresa financiera (la denominaremos a partir de ahora como Fincomp), la cual debe implementar un SOC por imposición de las nuevas políticas de seguridad que los bancos centrales imponen a sus clientes y entidades colaboradoras.

1.1.2 Justificación del proyecto

La realización de este proyecto viene motivada por los requisitos realizados por auditorías externas de las entidades reguladoras europeas a Fincomp para incrementar la seguridad y respuesta ante ataques externos y proteger la estructura financiera (un ataque en una entidad podría propagarse a todos los demás bancos y clientes conectados). Estas auditorías se llevan a cabo anualmente, y debido al aumento exponencial de ciber ataques a bancos y FMIs, el Banco Nacional ha decidido obligar a todas las instituciones a implementar un SOC.

La no implementación de éste daría lugar a la revocación de la licencia para operar en el país o con compañías pertenecientes a éste.

1.1.3 Motivación para realizar el proyecto

La idea para realizar este proyecto en concreto nace de la experiencia obtenida como Analista senior en un SOC desde hace 5 años en 3 empresas distintas; todas vinculadas al ámbito financiero.

Vinculado únicamente con la parte técnica; pero no en concreto con la implementación, sino con la respuesta a amenazas, este proyecto ayudará a mejorar el conocimiento en las diferentes áreas alrededor del SOC. Además, el conocimiento obtenido en el pasado se centra en el uso de Qradar, con lo que la implementación de Splunk en la red que se muestra en el proyecto, necesitará de investigación y un estudio previo, incrementando el conocimiento de esta herramienta para ser utilizada en el futuro y de cara a obtener posibles certificaciones asociadas ara progresar profesionalmente.

La administración de proyectos es un ámbito que se torna muy útil a la hora de adquirir conocimientos en el área de las TIC, de cara a un cambio laboral hacia una posición más de gestión que puramente técnica (Project Manager o SOC Manager, por ejemplo).

Para finalizar, una de las razones más importante es que el conocimiento y práctica de procedimientos de seguridad informática es personalmente muy interesante y unos de los más interesantes en el campo de las Tecnologías de la Información, y con una gran proyección de futuro tanto académico como profesional.

1.1.4 Contexto – Requisitos previos

A continuación, se enumeran los diferentes requisitos de los que la empresa dispone para poner en contexto el proyecto a realizar. Algunos aspectos no serán cubiertos en el proyecto, así que se asumirá que la Institución lo ha realizad por su cuenta; véase, por ejemplo, la contratación de empleados para cubrir las posiciones necesarias en el proyecto:

- Fincomp opera a nivel mundial, con diferentes sedes a lo largo de todo el mundo. Su sede central está localizada en Europa.

  Cada entidad está regida por las leyes del país donde opera, por ejemplo, en Europa toda la información tiene que cumplir con las directivas de la GDPR.

- La implementación se realizará completamente con equipos internos, apoyados por algún consultor externo para cumplir tareas específicas. Todos los empleados están ya en la empresa y tiene conocimientos de seguridad informática, pero no todos los tienen de las herramientas SIEM a desarrollar, por lo que un plan de enseñanza de las herramientas debe ser incluido en el proyecto.

- No se opera con Sistemas Front end de cara al usuario final (como ejemplo de estos sistemas, servicios de cajeros automáticos), sino que opera entre entidades bancarias mediante enlaces VPN, por lo que los accesos a la red están muy restringidos y solamente los empleados acceden mediante proxis específicos desde zonas de la red acotadas.

- Fincomp ya dispone de la infraestructura de red, en el proyecto se incluirá la parte de la red donde implementar el hardware SIEM y las conexiones con las

diferentes zonas y dispositivos para recoger los logs de éstas. Información más detallada de la red de la empresa se proporciona en la sección 2.7 de la memoria.

- La organización de la empresa y del SOC está establecida según el esquema de la figura 1:

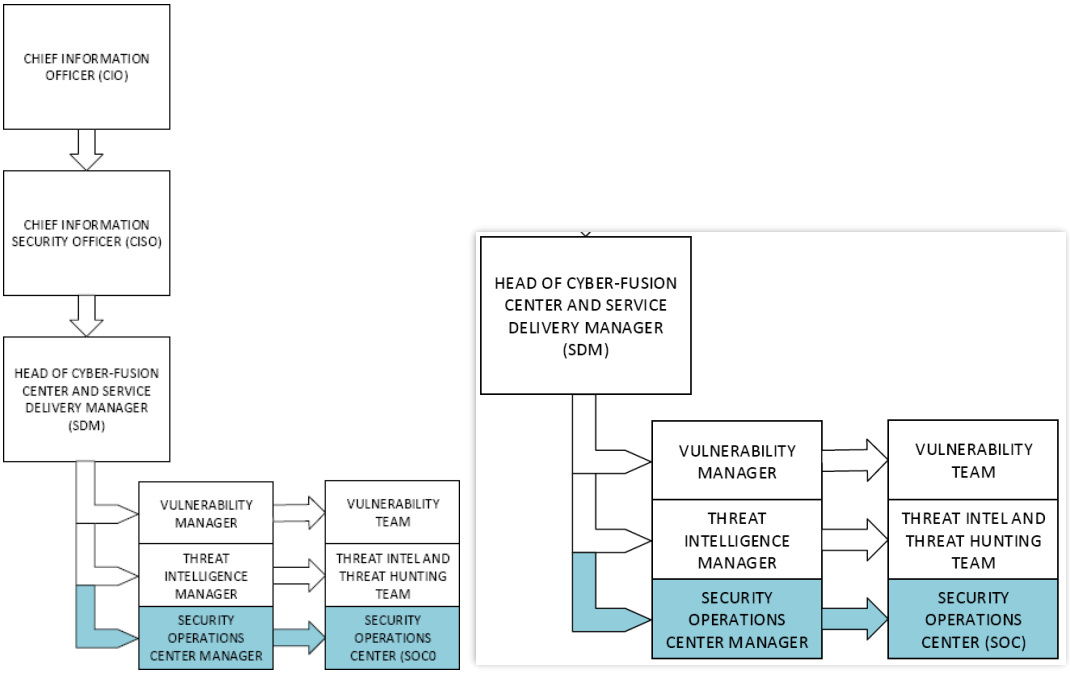


Figura 1. Esquema de la posición del SOC dentro de la organización. Se incluye la posición que tomaremos en este caso (SOC Manager).

Figura 1. Esquema de la posición del SOC dentro de la organización. Se incluye la posición que tomaremos en este caso (SOC Manager).

Como se aprecia en la imagen, la implementación de todo el SOC depende principalmente de la división de IT de la compañía y, a su vez, especializada en la sección de seguridad IT (con el CISO como director). Así mismo, se ha designado un mando intermedio para coordinar todo el Cyber Fusion center.

El Cyber-Fusion Center engloba todos los equipos que proporcionan monitorización y respuesta ante amenazas. No solamente está incluido el SOC, sino que también comprende los equipos de búsqueda de vulnerabilidades y parcheo, y los equipos que facilitan y distribuyen la inteligencia sobre las amenazas. En este proyecto solo se cubren los aspectos de SOC, ya que la inclusión del resto de secciones incrementaría la extensión del éste de manera considerable.

No obstante, estos equipos utilizarán las herramientas SIEM para sus investigaciones, por lo que la implementación planteada no cubrirá solamente las necesidades de un equipo, sino de múltiples dentro de la organización.

La posición que se toma en la realización de este proyecto es el punto de vista del Manager del SOC, ya que así se puede apreciar la visión de los múltiples aspectos de la implementación, pudiendo observar la parte técnica y la de gestión.

El SOC Manager será apoyado lateralmente por el responsable de servicios o Service Delivery Manager, el cuál interactuará con las demás secciones y departamentos de la empresa para obtener la ayuda en la implementación y creación de casos de uso (Use cases) requeridos por cada uno de ellos

Dentro del SOC distinguimos dos posiciones principales:

- Ingeniero del SOC: Son los responsables de instalar, mantener y actualizar las plataformas SIEM, así como de implementar las reglas y los casos de uso.

- Analista del SOC: Su labor principal es la de monitorizar las alertas generadas en la consola SIEM y responder adecuadamente a ellas en tiempo y forma. Se hace una distinción en este puesto entre analistas de primer nivel (Tier 1); con menos experiencia y conocimientos y analistas de segundo nivel (Tier 2) o senior. Estos analistas realizarán la verificación final y servirán de puente entre el SOC y otros equipos de respuesta.

- Las herramientas SIEM que se han aprobado para utilizar son Qradar y Splunk, las licencias ya han sido adquiridas y existe un contrato vinculante, no se puede optar por otro tipo de solución por el momento:

  - Qradar se utilizará como herramienta principal para monitorizar los casos de uso específicos y actuar. Monitorizará toda la infraestructura crítica de la empresa de forma progresiva, comenzando con la zona de test.

  - Splunk se utilizará como herramienta de soporte, y más específicamente para el uso por parte del NOC y de monitorización del tráfico de red.

  En las secciones 2.2 y 2.4 de la memoria se proporcionan más detalles al respecto de la elección de las herramientas SIEM.

1.2 Objetivos del Trabajo

Una vez clarificado el contexto, se van a describir a continuación los objetivos esperados y planteados al principio el proyecto. Estos puntos serán revisados en la sección 3 del proyecto para comprobar si, efectivamente, han sido alcanzados. En caso negativo, se verá la razón y como se podría completar en el futuro.

- El hardware y correspondiente software de las herramientas SIEM debe estar instalado como mínimo en la zona de test de la red, obteniendo eventos e información de todos los dispositivos y generando alertas. Como trabajo adicional, se va a intentar extender toda la solución a la zona de producción, pero se ha acordado que esto puede ser llevado a cabo por el equipo de ingenieros de forma progresiva en los siguientes seis meses a la finalización del proyecto.

- La disponibilidad del sistema implementado debe alcanzar el 99% del tiempo activo en la red; se debe diseñar una respuesta que asegure la completa

disponibilidad del sistema en poco tiempo, si se produce una caída (disaster recovery). Una configuración de alta disponibilidad debe ser implementada.

- Se debe entregar la documentación referente a toda la implementación de las soluciones SIEM, para ser utilizada por la compañía una vez que el proyecto finalice. No se requieren instalaciones paso a paso, pero si una visión general de la distribución en la red (la instalación la proporcionan las compañías del SIEM como soporte). Como mínimo se exige un 90% de la documentación necesaria en la fecha final.

- Se deben entregar una serie de procesos y documentación de como el SOC debe ser gestionado. Se acepta como mínimo un 90% del total.

- Se debe disponer de un plan de acción para responder ante las alertas generadas y los posibles incidentes de seguridad de acuerdo con el tiempo acordado por la empresa y los organismos externos. Se incluye:

    - Set de casos de uso acordados con los diferentes departamentos.
    - Reglas acordes con los casos de uso sugeridos.
    - Playbooks o libros de uso para actuar en consecuencia a las reglas creadas.

- Fincomp debe tener la capacidad y el conocimiento necesario para, al finalizar el proyecto, poder gestionar y hacer funcionar el SOC de forma autónoma. Para ello, debe ser propuesto un plan de entrenamiento para nuevos empleados y evaluado como viable por la dirección.

- Crear un sistema para informar mediante datos concretos de los progresos y avances en la implementación, así como de las estadísticas de incidentes creados, cerrados, escalados… para así responder a las posibles auditorias que evaluarán el nivel de madurez del SOC y su respuesta.

1.3 Enfoque y método seguido

Todos los aspectos descritos deben ser apoyados y entregados con su correspondiente documentación. Para documentar todas las tareas, procesos y demás, se ha optado por la herramienta Confluence (https://www.atlassian.com/software/confluence). Se proporcionan más detalles de la herramienta en la sección 2.4 de la memoria.

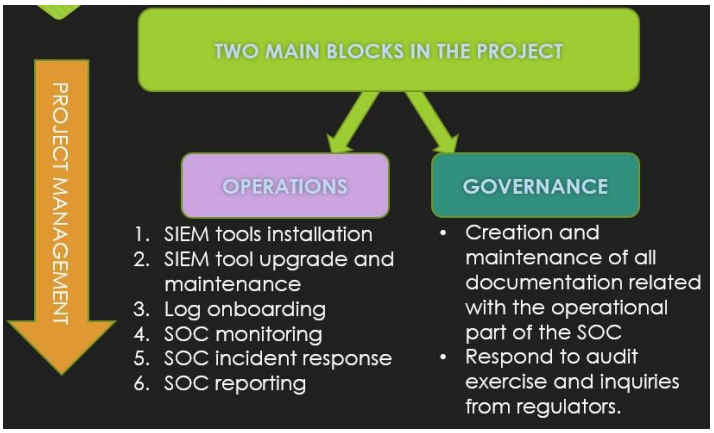


Figura 2. Representación esquemática del proyecto a realizar (en alto nivel)

El proyecto se realizará de una forma dual; tanto la parte de la implementación como de la gestión avanzarán a la vez, ya que muchos de los aspectos que se desarrollan en la documentación no requieren que la solución SIEM esté implementada. Realizar el proyecto de esta forma facilitará y agilizará la respuesta de éste y podrá ofrecer al cliente los entregables para verificarlos sin tener que esperar a la fase de cierre.

A su vez, la línea de tiempo del proyecto va a englobar tres partes diferentes. Se ha optado por una separación en tres partes, motivada por dos factores: el primero; como una forma de separar el trabajo y distribuirlo de forma más cómoda, asemejándolo a un proyecto real; y el segundo factor como una forma de distribución del trabajo de cara a la entrega de las diferentes PECs que acompañan a la memoria.

A continuación, se desglosa cada sección con el propósito de clarificar los aspectos tratados en cada una.

1.3.1 Operaciones

Este lado del proyecto se centrará en la parte más técnica, es decir, en la implementación del hardware y software, inclusión de la configuración en las herramientas, creación de cuentas y otros aspectos centrados en la parte de ingeniería y análisis.

Los principales aspectos a trabajar en esta parte serán los siguientes:

1. Instalación de las soluciones SIEM en la red del cliente, descripción de todos los requerimientos de hardware. Se asume que se dispone de suficiente presupuesto para llegar al mínimo de dispositivos necesarios.

2. Verificar el correcto funcionamiento y aplicación de actualizaciones si fuera necesario.

3. Agregar los logs de los dispositivos del cliente (endpoints, switches, firewalls…).

4. Crear las reglas para monitorizar los dispositivos agregados y los casos de uso requeridos por el cliente o los diferentes departamentos.

5. Crear los playbooks y casos de uso correspondientes, adaptándolos a las necesidades de tiempo y forma del cliente. Esta área cubre toda la respuesta a incidentes desde el principio hasta el final.

6. Crear estadísticas para reportar esta actividad a los puestos superiores y auditores de forma proactiva.

1.3.2 Gestión

La segunda parte es principalmente la parte que llevan a cabo los responsables del proyecto, en este caso el SOC manager y el Service Delivery Manager (SDM). Se centra en la documentación requerida y todos los procesos que envuelven el proyecto, como la creación de procesos de actuación.

1. Creación de toda la documentación referente al SOC.

2. Responder a las informaciones requeridas por las auditorias del cliente y externas.

3. Realizar la comunicación y toma de decisiones respecto a los aspectos del proyecto, realización del seguimiento del proyecto.

1.3.3 Metodología – Primera parte

IMPLEMENTACION INICIAL Y REUNIONES PARA DECISIONES: tiempo aproximado 45 días:

- La instalación de Qradar y Splunk comienza. en la red de test del cliente
- Verificación de la conectividad y creación de accesos a los miembros del SOC.
- Envió de logs de prueba a las soluciones SIEM.
- Testeo de reglas básicas para observar si todo funciona correctamente (test).
- Reuniones entre los miembros del SOC (managers) para acordar posibles modificaciones de fechas si fuera necesario, o cambios importantes después de la implementación (Reuniones semanales).
- Creación de borradores con las primeras documentaciones.
- Se comienza a crear el sistema de enseñanza para los nuevos analistas e ingenieros. No hay monitorización en este punto del proyecto.

1.3.4 Metodología – Segunda parte

SEGUNDA PARTE – COMIENZO DE LAS OPERACIONES Y LOS NUEVOS CASOS DE USO COMIENZAN A LLEGAR: tiempo aproximado 45 días

- La instalación debería haber finalizado en este punto; las modificaciones e instalaciones de parches empiezan en esta fase.
- Podría comenzar la instalación de aplicaciones específicas del SIEM si fuera necesario.
- Empiezan a llegar casos de uso de otros departamentos.
- Llegan las primeras auditorias para la revisión de documentos.
- Llegan las primeras alertas y son verificadas por los analistas; se espera respuesta a las mismas.

- Comienza la generación de estadísticas y reportes (semanales).
- Comienzan a llegar alertas generadas por los SIEM.

1.3.5 Metodología – Tercera parte

TERCERA PARTE – SISTEMAS FUNCIONALES EN PRODUCCION Y CIERRE DE PROYECTOÑ tiempo aproximado 20 días.

- Ingeniería finaliza instalación y se centra en la inclusión de casos de uso, solo actúa en el software en caso de incidente en el sistema.
- Auditoría se centra en la respuesta, verificando tiempos y detección.
- La documentación debe finalizar en este punto y debe ser utilizados por el SOC como base para proceder.
- Las operaciones deben funcionar de un modo independiente en este punto.
- Creación del cierre del proyecto y lecciones aprendidas.

1.4 Planificación del Trabajo

1.4.1 Software para la planificación

La planificación del trabajo se ha llevado a cabo utilizando dos herramientas de software diferentes.

- Para la creación de tareas y seguimiento se ha optado por la herramienta Trello. Mediante la inclusión de tarjetas con cada tarea, ayuda a organizar correctamente qué se debe hacer en cada momento, qué tareas están todavía incompletas y qué pasos se han completado.

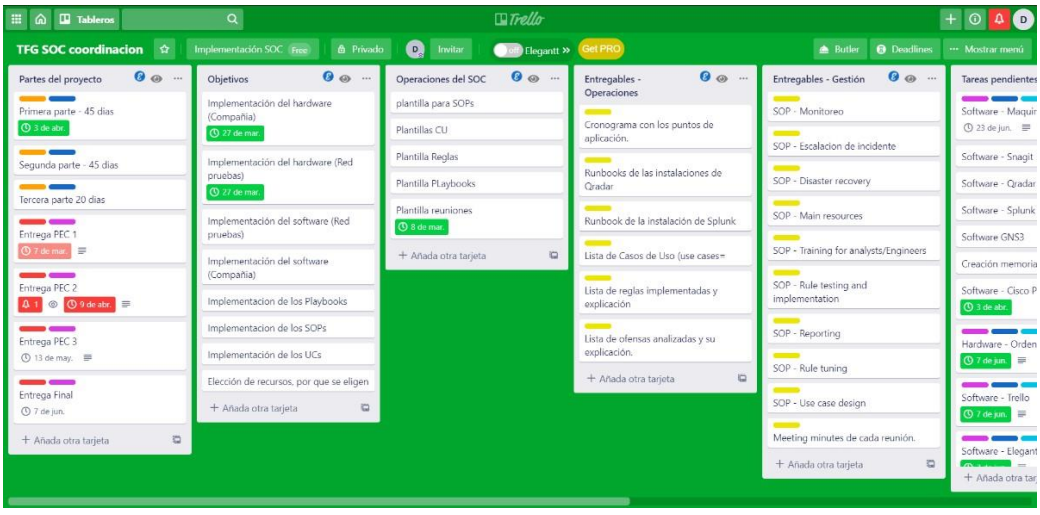


Figura 3. Vista del proyecto TFG SOC en Trello.

- La organización del proyecto se apoya en el uso de un diagrama de Gantt. Para su creación se ha recurrido a la herramienta Elegantt, la cual dispone de una extensión para Trello, por lo que podremos utilizar las tarjetas de éste para crear y modificar el diagrama.

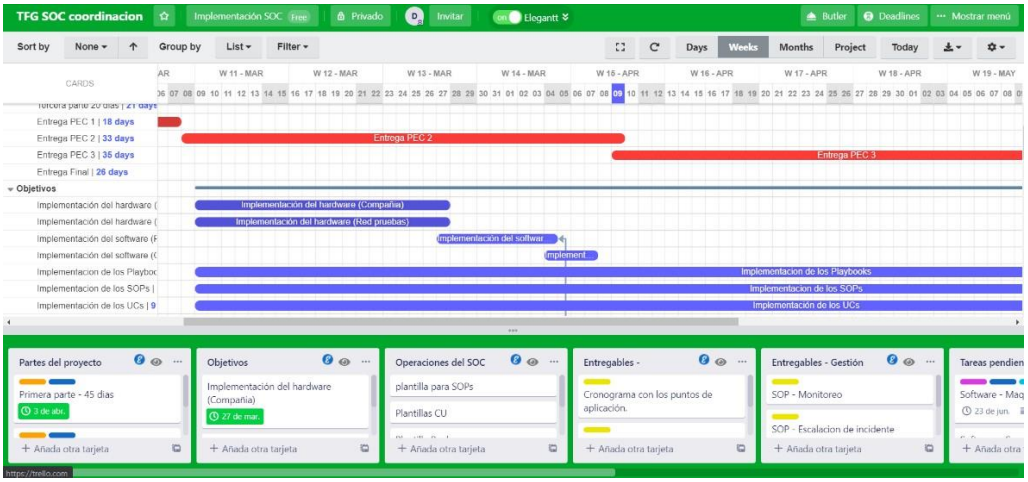


Figura 4. Implementación de la aplicación Elegantt al proyecto SOC de Trello.

1.4.2 Diagrama de Gantt y explicación de objetivos

Para la muestra de cómo se ha distribuido el tiempo en el proyecto se ha incluido el diagrama de Gantt obtenido mediante Elegantt. Se ha considerado como fin del proyecto la fecha de entrega de la memoria; aproximadamente 7 de junio.

El cronograma completo se encuentra en la sección 6.1 del anexo de la memoria.

Como se observa en el diagrama proporcionado, se han establecido una serie de dependencias entre tareas, ya que, por ejemplo, no se pueden introducir los eventos de los logs en las herramientas SIEM si no disponemos de éstas instaladas en el sistema. O con la creación de los procedimientos si no se dispone de las plantillas creadas para ello en Confluence.

El color de las Tareas viene principalmente indicado por las etiquetas que cada parte del proyecto tiene. Por ejemplo, se ha tomado el color amarillo como tareas que proveen de entregables, o el color rojo para indicar tareas que han sido canceladas (se explicará el por qué más adelante en la memoria). Se ha optado por esta clasificación debido a que se pueden localizar las tareas de una manera muy visual.

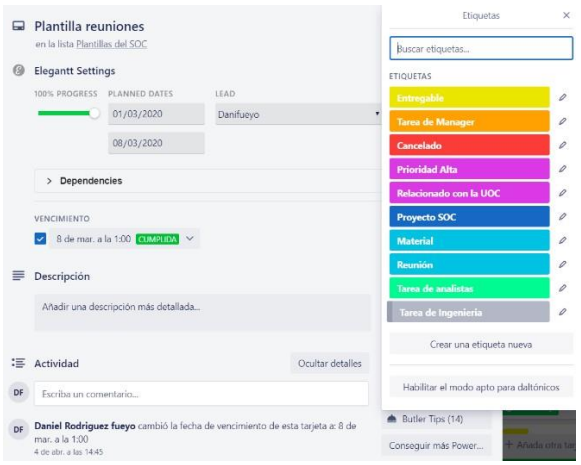


Figura 5. Ejemplo del uso de las etiquetas en la organización de las tareas. Visualización de las etiquetas creadas

1.4.3 Planificación dividida por PECs

La planificación que se ha optado para cada una de las PECs va en consonancia con las tres fases en las que se divide el proyecto; aunque alguna modificación se ha realizado durante el proyecto, por lo que no es una coincidencia al 100% con el desarrollo del proyecto. Se desgrana a continuación lo que se espera entregar en cada una de las PECs:

- **PEC 1: Propuesta del plan de trabajo**

  Se desgrana la explicación del proyecto a realizar, explicando los conceptos relevantes, materiales y cómo se procederá con la organización.

- **PEC 2: Introducción, primeras instalaciones y decisiones**

  En esta PEC se debe finalizar la implementación de la red de pruebas y la configuración de la red del cliente. Se deben finalizar las plantillas para la creación de los documentos de gestión y la configuración de todo el software y hardware necesario para proceder con el proyecto. La red de pruebas debe contener la instalación de las dos herramientas SIEM. Se debe calcular el coste de implementación de las soluciones SIEM en la red del cliente, no de todo el proyecto, lo cual será en otra fase.

- **PEC 3: Finalización de la parte técnica, creación de documentación y pruebas de funcionamiento.**

  Con la red ya implementada, se entrará en la configuración específica de las soluciones SIEM, la cual incluye el envío de los logs dentro de éstas, la configuración de cuentas y la generación de reglas acorde.
  Por la parte que concierne a las operaciones; se procederá a la creación de todos los procedimientos requeridos a partir de las plantillas obtenidas y las decisiones en las reuniones del equipo. La creación de los casos de uso, reglas y libros de reglas vendrá supeditada a la configuración correcta de los SIEM, ya que es necesaria la interacción con las herramientas para completarlos.

- **PEC 4: Cierre de proyecto, conclusión, coste y entrega de memoria.**

Esta PEC es la que se correspondería, en un proyecto real, con la fase de cierre del proyecto. Se va a calcular el coste del proyecto, terminar la documentación pendiente si la hubiera y comprobar si los objetivos y entregables han sido completados exitosamente.
Se deberá proceder con la conclusión del proyecto y la finalización y revisión de la memoria a entregar. Se deberán incluir los anexos relacionados con la documentación creada para el cliente.

1.5 Breve sumario de productos obtenidos

A continuación, se muestra la colección de entregables a proporcionar al cliente, las diferentes partes interesadas (stakeholders u otras divisiones) y las diferentes auditorias que se realicen durante el proyecto.

1.5.1 Entregables (Operaciones)

- **Para validar el proyecto:** Diagrama de Gantt con las implementaciones incluidas y las operaciones realizadas, incluyendo fechas clave, reuniones, y entregables.

- **Para la implementación:**

  La documentación se entregará como anexos creados con la aplicación Confluence:

  - Entrega de todos los procedimientos y proceso relativos a la gestión de las soluciones SIEM.
  - Entrega de los casos de uso creados o plantillas relacionadas.
  - Entrega de la documentación de las reglas creadas.
  - Entrega de los Playbooks creados y verificados.
  - Entrega de reportes con las estadísticas de las operaciones.

1.5.2 Entregables (Gestión)

- **Procesos y SOPs:**

De nuevo, toda la documentación mencionada se entregará como anexos obtenidos mediante Confluence.

- Disaster recovery plan para el SOC: Plan para responder ante una interrupción del servicio de monitorización.

- Monitorización de alertas: Cómo realizar una monitorización correcta de las alertas generadas en los SIEM

- Escalación: Cómo proceder en caso de que una alerta generada sea clasificada como un potencial incidente de seguridad.

- Modificación de reglas: Pasos para modificar correctamente una regla existente en los SIEM

- Creación de casos de uso (UC): Pasos para la creación estandarizada de casos de uso.
- Creación de reglas (RC): Pasos para la creación estandarizada de reglas en los SIEM.
- Creación de playbooks (PC): Pasos para la creación estandarizada de libros de reglas.
- Creación de reportes **(Cancelado – no depende del SOC):** Creación estandarizada de reportes y estadísticas.
- Plan de enseñanza para miembros del SOC: Pasos de entrenamiento para los nuevos analistas que comiencen en el SOC.

Toda la documentación referente a las reuniones que se produzcan durante el proyecto, por razones de verificación y responsabilidad en las decisiones tomadas.

1.6 Breve descripción de los otros capítulos de la memoria

Para la completa implementación inicial del SOC, se ha optado por una división de capítulos en la memoria que se corresponden cronológicamente con las fases del proyecto realizadas, para así conseguir que todos los pasos puedan ser contrastados con la organización de éste y no creen confusión

1.6.1 State of the Art

Se ha incluido el estado del arte en la memoria del proyecto, ya que se explican los avances actuales dentro de los SOC y la forma de actuación de los posibles atacantes a las redes de grandes compañías. Sirve como una introducción al proyecto a tratar, y da contexto a lo que se explica en los siguientes capítulos.

1.6.2 Elección del hardware para el proyecto

Este capítulo desgrana la elección de hardware que se empleará en la realización del proyecto, ya sea en la zona de pruebas o en la compañía en sí y por qué se ha elegido éste en concreto y no otro.

1.6.3 Implementación del hardware

Una vez enumerado y explicado del hardware, se dará una breve descripción de cómo se ha utilizado en el proyecto. No se entrará en detalles específicos para no alargar el contenido.

1.6.4 Elección del software para el proyecto

En este capítulo se incluirá todo el software utilizado durante la realización del proyecto, incluyendo las soluciones SIEM. Se explicará, al igual que con el hardware, el porqué de la elección en cada caso.

1.6.5 Implementación del software

Se procederá a la explicación de los pasos generales de cómo se ha implementado o qué uso específico se le ha dado a cada elemento.

1.6.6 Planteamiento de la red de pruebas y configuración

Se desgranará en este capítulo como se ha planteado la red de pruebas para el proyecto, incluyendo el diseño lógico y la comprobación de que la comunicación entre todos los elementos es la correcta.

1.6.7 Planteamiento de la red en la empresa

Se esquematizará el diseño general de la red de la empresa donde se implementarán las soluciones SIEM, se dará una introducción a cada una de las zonas, explicando qué elementos se encuentran y cómo se monitorizarán y enviarán los logs para monitorizarlos.

1.6.8 Plan de recuperación ante desastres (disaster recovery)

Explicación del funcionamiento y configuración del plan de continencia ante desastres elaborado. Se adjuntará el procedimiento correspondiente en la sección de anexos.

1.6.9 Creación del acceso granular para los miembros del SOC

En esta parte de la memoria se procederá con la explicación general (no paso a paso) de como se ha conseguido la configuración del acceso granular a Qradar y Splunk, para facilitar el uso de las herramientas por los empleados del SOC.

1.6.10 Plan de entrenamiento para nuevos analistas

Se dará una explicación en este capítulo de la organización y entrenamiento para los nuevos empleados que sean contratados en el SOC. Se ha creado un documento correspondiente e incluido en los anexos.

1.6.11 inclusión de los registros en las herramientas SIEM (log onboarding)

El proceso de envío de los eventos generados en las máquinas de la red será definido en este punto. Se incluye una explicación para la zona de pruebas y su equivalente en la red de la empresa.

1.6.12 creación de los casos de uso (Use cases)

Este capítulo se divide en dos partes. Uno es el del procedimiento correspondiente a la creación de los casos de uso, y el otro engloba la creación de casos de uso específicos para la red de la empresa, los cuales se generarán y probarán en la red de pruebas. Se mostrarán cinco ejemplos de casos de uso creados para la empresa.

1.6.13 Configuración de las reglas acordes a los casos de uso.

Una vez completado el capítulo anterior, con los casos de uso específicos creados, se procederá a crear reglas en los SIEM acordes a ellos, para poder monitorizar y responder antes estas posibles amenazas en la red. Se adjuntarán las reglas específicas creadas y la documentación asociada en los anexos.

1.6.14 Creación de los Playbooks para los analistas

Para continuar la construcción en cascada, se describirá la definición de un libro de reglas, el procedimiento para crearlos y los cinco ejemplos equivalentes a cada una de las reglas de la red creadas para este fin.

1.6.15 Plan Testeo de reglas y respuesta con casos reales

Cuando se dispone de todos los elementos para detectar y analizar las ofensas, se mostrarán cinco casos que activen los casos de uso mencionados y observaremos una posible respuesta a cada uno por parte de los analistas; para comprobar si todos los procesos creados pueden ser ejecutados correctamente.

1.6.16 Estadísticas e informes para directiva y auditoria.

En este capítulo, una vez obtenidos todos los datos, explicaremos brevemente cómo responder antes una petición de datos por parte de un equipo externo de auditores. Para proporcionar los datos requeridos se utilizarán las potentes herramientas de estadísticas y reportes que poseen ambos SIEM, las cuales simplificarán inmensamente la labor, procediendo a la automatización.

1.6.17 Valoración económica del trabajo

Dividiremos este capítulo en dos secciones principales: En la primera sección se crearán presupuestos solamente para la incorporación de las soluciones SIEM en la infraestructura (hardware y software), ya que será la parte del presupuesto más abultada; una vez completadas las estimaciones de coste de las SIEM, se creará un presupuesto global, incluyendo posibles horas de trabajo y previsiones de gasto adicional.

1.6.18 Cierre del proyecto

En el momento de la finalización del proyecto, se desgranará en este capítulo como se producirá la transición entre el final del proyecto y la continuación de las operaciones implementadas por parte del cliente, ya que este proyecto es solo la fase inicial de

implementación. A partir de este punto el trabajo debe continuar por parte del cliente de forma autónoma.

Se incluirán también los puntos del proyecto que no han sido llevados a cabo o retrasados, exponiendo las razones de ello.

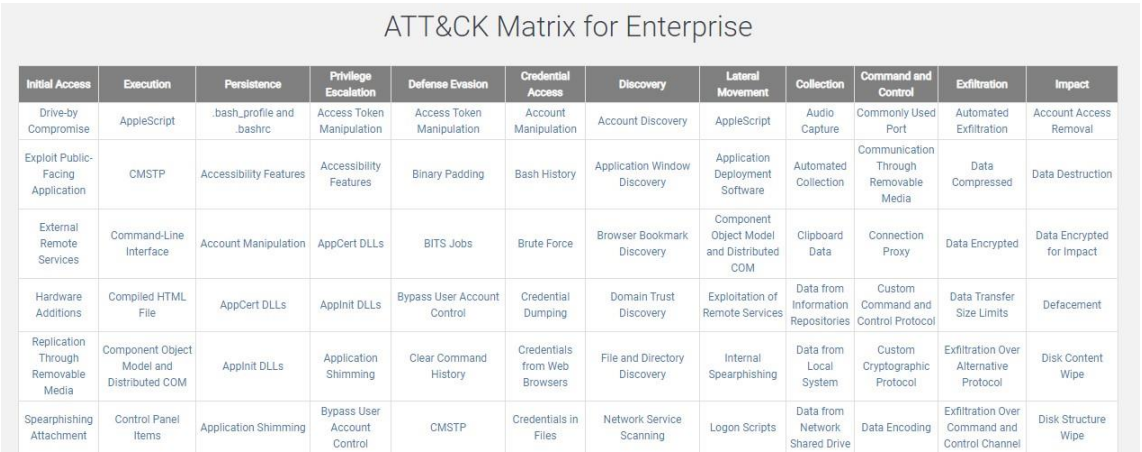
2. Resto de capítulos

2.1 State of the Art

2.1.1 Ciber amenazas y Actores

Múltiples amenazas de ciber seguridad están activas hoy en día para todo el mundo, pero, es especialmente para las empresas, y más en concreto para las instituciones financieras, donde este riesgo aumenta, ya que los grandes ¨actores¨ especializados en ciber ataques, centran sus actividades en ellas.
Obviamente esto tiene todo el sentido, ya que estas grandes y poderosas organizaciones, muchas de ellas mantenidas y entrenadas por países (véase Corea del Norte con Lazarus), van en busca del dinero o, mejor dicho, de los lugares donde pasa el dinero.
Esto se ha podido observar en los últimos años con las acciones perpetradas por ejemplo por Lazarus, atacando las infraestructuras de transferencias SWIFT en bancos situados en países del sudeste asiático con bastante éxito.

Las actividades incluidas en el modus operandi de estos grupos son seguidas activamente por los servicios secretos y las agencias de inteligencia de todo el mundo, sus técnicas (como la inyección Powershell o las campañas Maldoc) son documentadas y se pueden encontrar en el framework MITTRE ATT&CK (Figura 2), que es una de las principales bases de datos a seguir en las operaciones diarias de un SOC.



ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Replication Through Removable Media	Component Object Model and Distributed COM	AppInit DLLs	Application Shimming	Clear Command History	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Spearphishing Attachment	Control Panel Items	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe

Figura 6. Ejemplo de una de las matrices del modelo ATT&CK para empresas, donde se pueden ver las técnicas más utilizadas por los grandes grupos de hackers.

2.1.2 Herramientas SIEM

Como mucha gente sabe, el campo de la ciber seguridad es relativamente nuevo, pero desde ya más o menos una década, grandes compañías trabajan para desarrollar soluciones para luchar contra este tipo de amenazas.
Las soluciones que se han elegido para aplicar como herramientas SIEM han sido Qradar (IBM) y Splunk. Esta elección no ha sido aleatoria, ya que como se puede apreciar en el cuadrado mágico de Gartner del año pasado (Figura 3), ambos se encuentran a la vanguardia del mercado de las tecnologías SIEM hoy en día.

Figura 7. Cuadrado mágico de Gartner donde se incluyen las herramientas SIEM del mercado y su posición en este (último dato generado en febrero de 2020)

2.1.3 Últimos avances en los SOC

Los SOC alrededor del mundo están viviendo una rápida evolución, una de las metas en las que las empresas se centran es en la automatización y la implementación de Inteligencias artificiales para la asistencia de los analistas y consultores, debido principalmente a la ingente cantidad de información que se maneja.
Una de las herramientas más prometedoras es una IA desarrollada por IBM con el nombre de WATSON. Esta IA monitoriza las actividades de grupos internacionales, comparando el tráfico con éstas y el framework MITRE y otras fuentes de información externas para ayudar en la detección de posibles intrusiones en la red de acuerdo con todos los parámetros configurados.

Además de estas, existen otras tecnologías usadas en otros ámbitos que se están adaptando al uso de los sistemas SIEM, como son las siguientes:

- User Behavior Analysis.
- Endpoint protection
- Inserción automática y reconocimiento de dispositivos en la red.

- Machine Learning y Big Data aplicado a los SIEM.

2.2 Elección del hardware para el proyecto

Una de las tareas iniciales a la hora de plantear la construcción del SOC (y de muchos otros proyectos), es la de elegir el hardware y software apropiado para cada ocasión, ya que el tiempo empleado y el coste pueden variar drásticamente debido a este factor. Por ello se van a explicar en este capítulo qué elementos de hardware vamos a necesitar para nuestro proyecto, y el porqué de le elección de este producto específicamente.

2.2.1 Herramientas SIEM: Qradar y Splunk

El mercado de los SIEM, como los SOC, ha experimentado un rápido crecimiento. Hoy en día se dispone de muchísimas soluciones diferentes, tanto de uso bajo licencia comercial (de pago), como SIEM de código abierto. Algunas de las soluciones SIEM más famosas del mercado son las siguientes:

- SIEM de código abierto: AlienVault OSSIM, Snort, Elasticsearch
- SIEM bajo licencia comercial: RSA SIEM, ArcSight, Splunk, QRadar

En nuestro caso se ha optado por descartar directamente las soluciones de código abierto, no porque sean peores, sino porque en el caso de la implementación en la red del cliente, se necesita proveer do soporte a la solución las 24 horas del día, y esta característica solamente estás disponible para los SIEM bajo licencia comercial.

Una vez nos hemos decantado por las soluciones de pago, se ha optado por una solución mixta, no de un solo producto sino de dos. Esta elección viene por varios motivos:

1) Tener dos SIEM diferentes nos provee de dos formas combinadas de trabajo distintas, pudiendo dividir las alertas por tipos y no tener que saturar la consola y el sistema de una sola.
2) Las licencias para monitorización de los SIEM crecen exponencialmente dependiendo del número de eventos o capacidad recibida en ellos: Separando parte del tráfico de la red en dos soluciones distintas, nos permite utilizar menos porcentaje de ancho de banda, limitando el valor de la licencia que se debe adquirir
3) En caso de emergencia y no poder recuperar el acceso a una de las herramientas, el envío de la información puede sr desviada al segundo SIEM temporalmente, mitigando la desconexión y consiguiendo que la disponibilidad de la monitorización se mantenga.

Cuando ya tenemos definido el número de soluciones y el tipo, falta la elección específica del producto. La empresa Fincomp se ha decantado finalmente por la obtención de los sistemas pertenecientes a Qradar (IBM) y Splunk. Hay varias razones de esto, algunas puramente de marketing (las grandes empresas detrás de un producto suelen dar confianza extra), pero la principal ha sido que estos dos productos, pese a ser claros rivales en la lucha por el mercado, se complementan muy bien juntos:

- Qradar es una herramienta que funciona de manera muy intuitiva y con una interfaz gráfica muy potente y enfocada a los analistas, no es tan complicada como otras soluciones (Arcsight por ejemplo es bastante difícil de interpretar si no se dispone del conocimiento técnico suficiente)

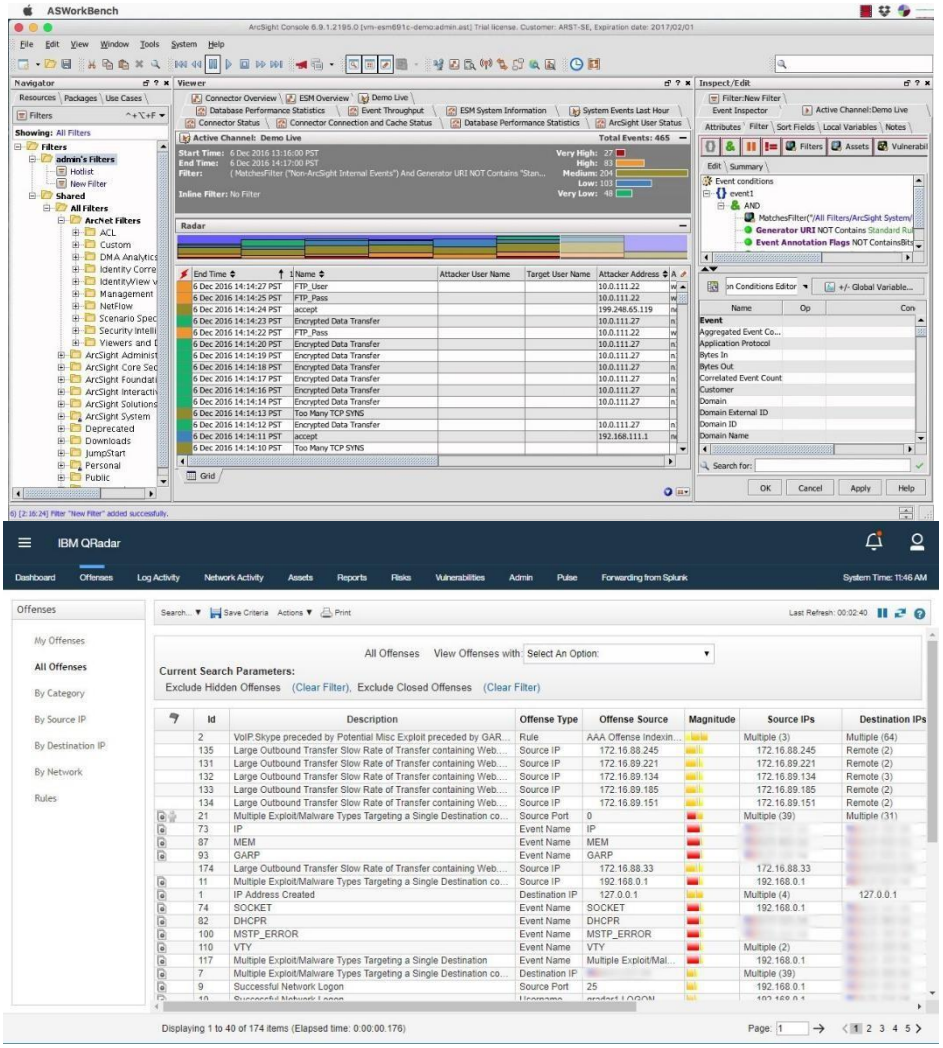


Figura 8. Comparación entre la interfaz de Arcsight (arriba) con la interfaz de Qradar (abajo), la interfaz de Qradar es mucho más intuitiva.

- Splunk es una solución mucho más enfocada a la automatización, sirviendo también como capturador de paquetes y tareas más específicas de red.

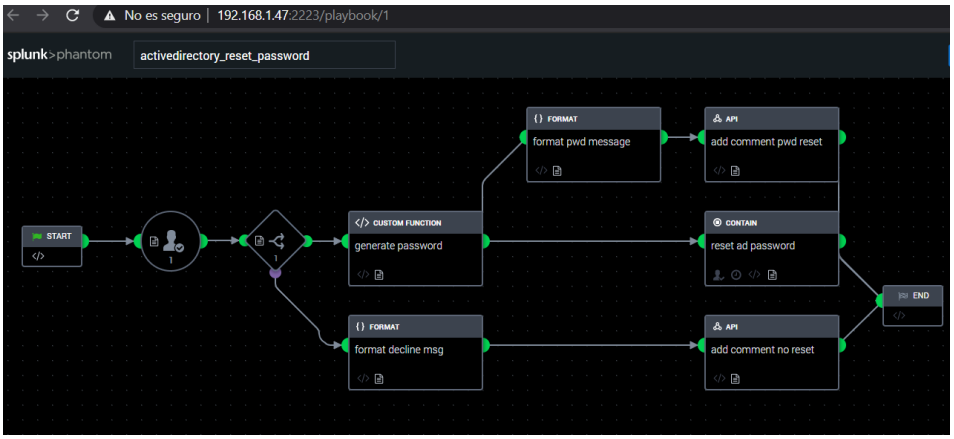


Figura 9. Ejemplo de la automatización de un libro de reglas con Splunk (playbook).

- Ambos están configurados para obtener los logs de una solución a otra sin necesidad de configuraciones adicionales (lo traen configurado por defecto u out-of-the-box).

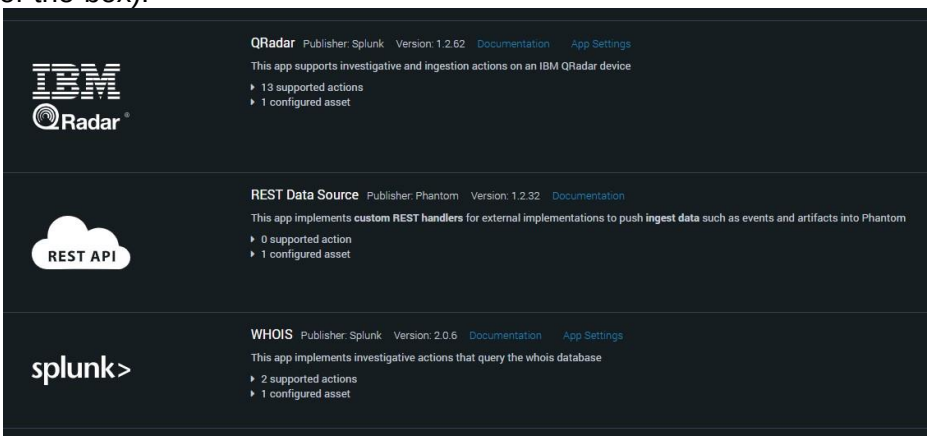


Figura 10. Aplicación en Splunk para incluir los eventos directamente de Qradar, incluso exportar las reglas directamente. Se incluye una opción para incluir eventos de otro Splunk.

Por todo lo explicado antes e incluyendo algunas decisiones tomadas desde la dirección fuera del SOC (el presupuesto se asigna desde el Consejo de Administración) se ha optado por estas dos soluciones, complementarias entre sí.

Cabe mencionar que se supone que la empresa dispone de todos los elementos de red adquiridos, instalados y configurados, al igual que proveerá a los analistas con el hardware necesario para poder desempeñar sus labores de forma autónoma y regular.

2.2.2 Hardware para la red de pruebas: Ordenador portátil.

Para la red de pruebas, donde realizaremos todas las implementaciones de prueba y test de respuesta, se ha necesitado simplemente de un solo ordenador portátil, este dispositivo va a poder generar, junto con Virtualbox, una red virtual con NAT a la red de casa, la cual dará el enlace a Internet necesario para hacer funcionar todo correctamente. El ordenador en concreto es un Lenovo P50.

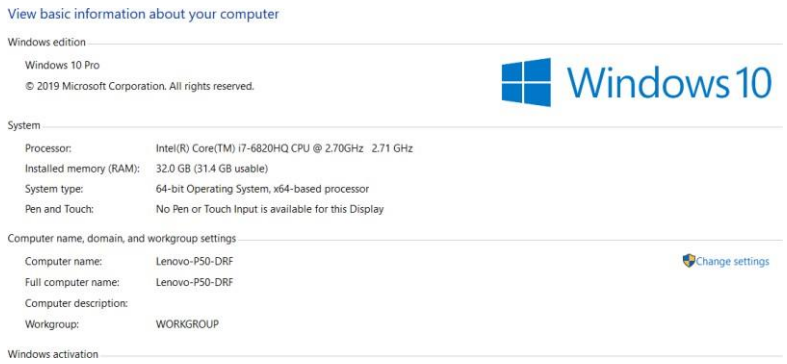


Figura 11. Información del sistema obtenida del propio ordenador

La principal ventaja y lo que ayudará en la consecución del proyecto de una manera más eficiente es la cantidad de memoria RAM (32 GB); Qradar y Splunk funcionando de manera virtual requieren un mínimo de 20 GB de memoria RAM entre ambos, por lo que no poseer tanta capacidad de memoria complicaría la creación de la red, teniendo que disponer de terminales físicos extra (otros ordenadores probablemente) conectados a la red para poder mantener todo el sistema funcionando a la vez.

2.3 Implementación del hardware

Vamos a centrarnos para la implementación del hardware en la implementación de los dispositivos SIEM en la red. De la red de pruebas no hablaremos en este caso, ya que el ordenador no requiere de ninguna implementación de hardware; todo el trabajo se realiza mediante software.

No se va a entrar en mucho detalle sobre la implementación de las soluciones SIEM, ya que esto se explica de una forma más sencilla junto con la explicación del diagrama de red de ésta, ahí se verán que dispositivos se deben colocar en cada sección para obtener la cobertura de red deseada.

Lo que sí vamos a explicar es cómo funciona el hardware de las soluciones SIEM de forma general, aplicable a Qradar y Splunk.

Los SIEM funcionan normalmente obteniendo eventos y logs de otras aplicaciones, por lo que basta con tener estos redireccionados correctamente al SIEM, pero obviamente se necesita que el SIEM ¨vea¨ la ruta hasta esos dispositivos.

Si nos encontramos con una infraestructura en la que hay diferentes rangos de red, necesitamos aparte del servidor SIEM principal, otros dispositivos de hardware, normalmente denominados colectores de logs (log collectors); estos dispositivos se encargan de almacenar directamente todos los eventos de una zona y comunicarse con el servidor principal para enviárselos al servidor SIEM. Cada uno de estos colectores es un servidor extra, normalmente con gran capacidad de almacenamiento, para retener gran cantidad de información e ir enviándola en los intervalos configurados para ello.

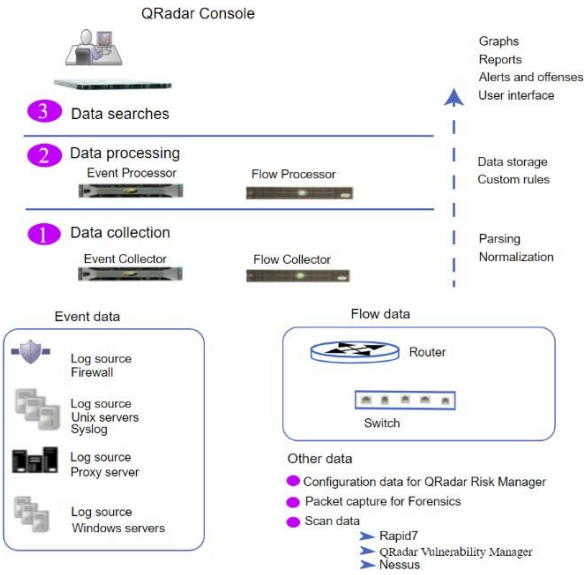


Figura 12. Esquema de la implementación de hardware SIEM, en este caso Qradar. fuente

Existe un dispositivo extra en caso de grandes infraestructuras, que se coloca paralelamente al servidor principal SIEM, y es el denominado procesador de logs (Log processor); este dispositivo de hardware se encarga de liberar al servidor principal de la tarea de procesar la información y ordenar los eventos de forma entendible para el analista.

En este caso, para nuestro proyecto necesitaremos de la infraestructura completa descrita. Nos centraremos en este proyecto en los logs para Qradar, dejando los flows (generados por dispositivos de red) para Splunk.

2.4 Elección del software para el proyecto

Si bien se ha visto que el hardware no es muy numeroso en el proyecto que nos concierne, no es el caso del software. Tanto la parte de implementación en la empresa como en la red de pruebas, se utilizarán múltiples herramientas de software para monitorizar, reportar y crear documentación, se irán explicando a continuación uno a uno:

2.4.1 Qradar (red empresa) y Qradar Community Edition (red de pruebas)

Como se mencionó en el capítulo del hardware, una de las soluciones SIEM implementadas será Qradar.

Para la red se ha optado por la versión 7.3, la cuál es la más estable por el momento. Existen versiones más actuales1 (7.3.3 o 7.4), pero se han reportado errores notables que podrían dificultar la implementación y dar errores en la instalación inicial.
Esta versión es final y posee todas las características acordes a la licencia de IBM, como son la inclusión de infinidad de colectores de logs, eventos ilimitados (dependiendo de la licencia adquirida) y la posibilidad de instalar cualquier App extra en el SIEM.

[1] Para ver todas las versiones disponibles de Qradar, véase: https://www.ibm.com/support/pages/qradar-master-software-version-list-release-note-list-updated

La licencia adquirida en este caso cubre la generación de 25000 eventos por segundo (EPS), se desgranarán más detalles de la licencia en la sección de presupuesto.

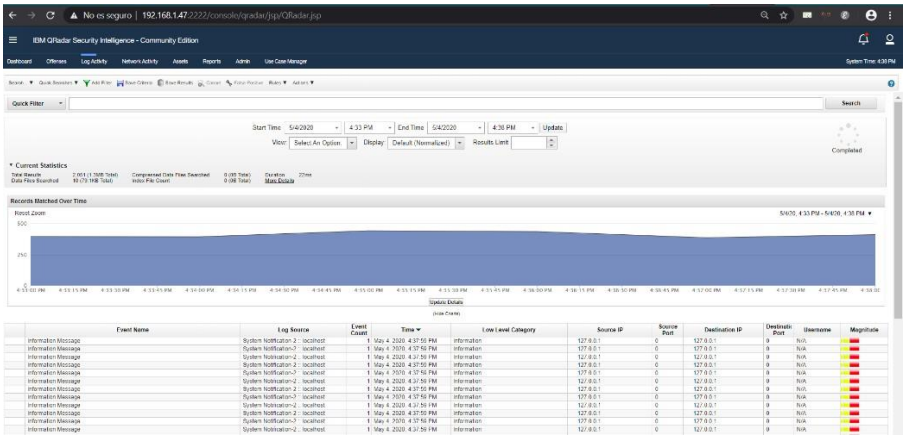


Figura 13. Imagen de la aplicación Qradar Community Edition, versión 7.3.3 (la versión utilizada en la red de pruebas.

En la red de pruebas se ha optado por la versión de Qradar Community Edition. Esta versión es gratuita, pero se encuentra limitada a 500 eventos como máximo por segundo, y solamente se puede utilizar un colector local (cada colector requiere de una pieza de hardware adicional). Para su ejecución en la red de pruebas se ha extraído un archivo de imagen de Virtualbox disponible desde la página de IBM.

2.4.2 Splunk (red empresa) y Splunk Phantom (red de pruebas)

El mismo concepto aplicado a Qradar se utilizará para Splunk. En este caso se utilizará la última versión disponible (8.0) para implementar en la red del cliente, mientras que en las red de pruebas se utilizará Splunk Phantom.

Splunk Phantom es la versión gratuita para estudiantes e investigadores de Splunk, viene limitada, pero contiene todo lo necesario para poder ser utilizada correctamente en la red de pruebas como equivalente del producto final en la red de empresa.

Existe otra versión de Splunk gratuita, denominada Splunk Free, pero esa versión no contiene, entre otras cosas, la posibilidad de crear y administrar cuentas de usuario, o de monitorizar alertas (básico para nuestro proyecto).

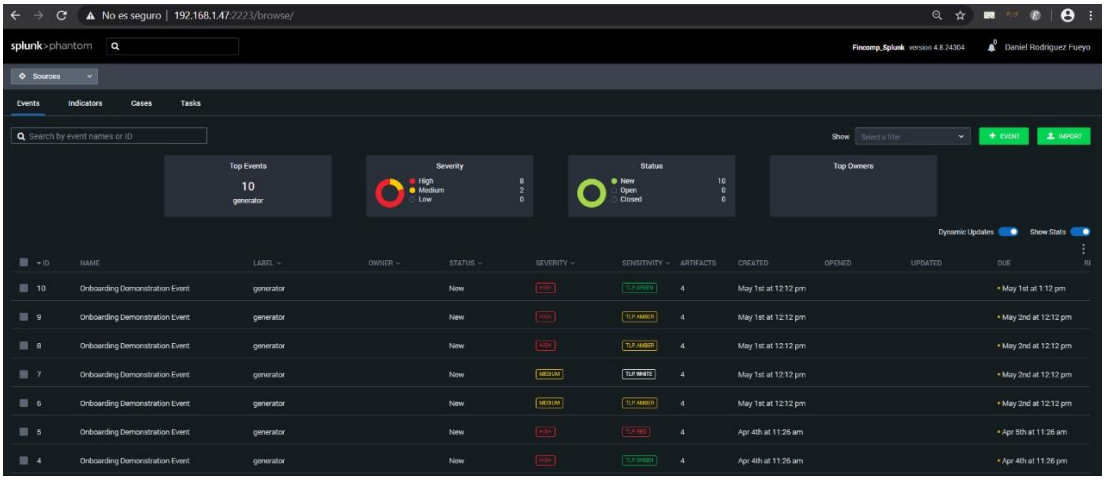


Figura 14. Captura de pantalla de la interfaz gráfica para alertas en Splunk Phantom (red de pruebas).

La versión de Splunk Phantom instalada será la versión 4.8.24304 y aunque en esta versión no se pueden incluir fuentes de eventos directamente, serán enviados a través de Qradar, por lo que las alertas serán recibidas de la misma manera.

2.4.3 Oracle VM VirtualBox Manager (Red de pruebas)

Se utilizará Virtualbox para realizar la virtualización de todos los elementos de la red de pruebas, ya que obtener hardware real para hacer las pruebas sería altamente costoso, tanto en tiempo como en presupuesto. Gracias a Virtualbox se ha podido recrear una red a pequeña escala con ambos SIEM funcionando simultáneamente para monitorizar 2 diferentes máquinas virtuales, todas obtenidas de manera gratuita y emuladas a través de Virtualbox.

El programa se ha obtenido de forma gratuita en la web oficial de Virtualbox, la versión utilizada para el proyecto ha sido la versión 5.2.16 r123759 (Qt5.6.2)

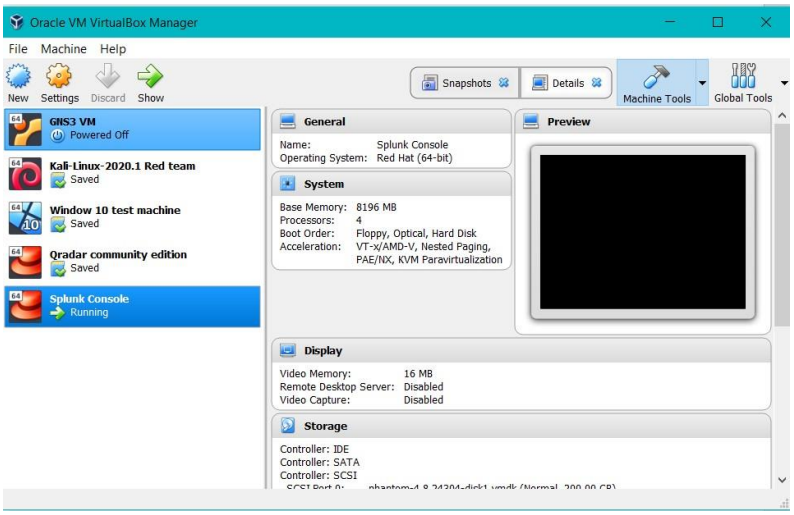


Figura 15. Máquinas virtuales instaladas para la red de pruebas del SOC en Virtualbox.

Existen otros programas de emulación alternativos, como puede ser VM Ware, pero muchos de ellos requieren versiones de pago para las máquinas virtuales de los SIEM, en el caso de Virtualbox, estas se proveen de forma totalmente gratuita, y preparadas directamente para ser instaladas.

Otra razón adicional para la selección de este programa en lugar de otros más conocidos es que ya se había trabajado con él en el pasado, incluso en algunas asignaturas impartidas en la UOC.

2.4.4 Máquina Virtual Windows Pruebas

Como es uno de los mayores sistemas operativos utilizados en el mundo, una de las máquinas virtuales utilizadas para la prueba de alertas es una maquina Windows, con la versión de Windows 10 instalada. Esta máquina virtual está disponible de forma gratuita a través de la web de desarrolladores de Microsoft.

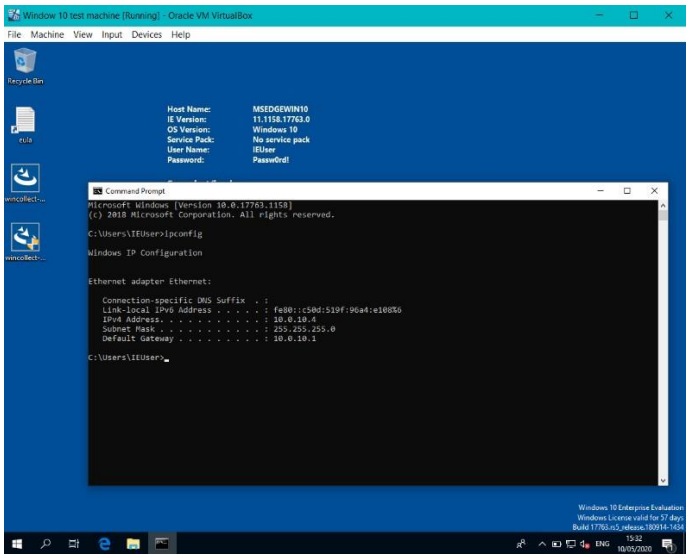


Figura 16. Visión del escritorio de la máquina de prueba de Windows 10 con su IP asignada en la consola de comandos.

Al poseer el ordenador portátil sistema Windows 10, cabría la duda de que podría haber sido utilizado para las pruebas, en lugar de instalar una máquina específica. Pero debido a las pruebas con software potencialmente malicioso, es una buena práctica hacerlo en una máquina virtual, la cual sirve a la vez como máquina Sandbox, sin afectar al ordenador sobre el que se ejecuta todo, pudiendo poner en riesgo la integridad de los datos.

Esta máquina virtual dispone de una licencia de 90 días y funcionalidad total de la versión Windows 10, pudiendo testear posibles ataques y modificaciones en el sistema sin riesgo para la red.

2.4.5 Máquina Virtual Kali Linux – Red team

Una vez que disponemos de una máquina de pruebas, necesitamos una máquina que actúa como agente externo ¨malicioso¨ para intentar acceder o sabotear la red, y comprobar así si el sistema genera las alertas deseadas y la actividad no pasa inadvertida para los SIEM.

Para realizar este trabajo se ha optado por instalar una máquina virtual Linux Debian Kali Linux, la archiconocida distribución para realizar pentesting o auditoria de redes mediante (hacking ético).

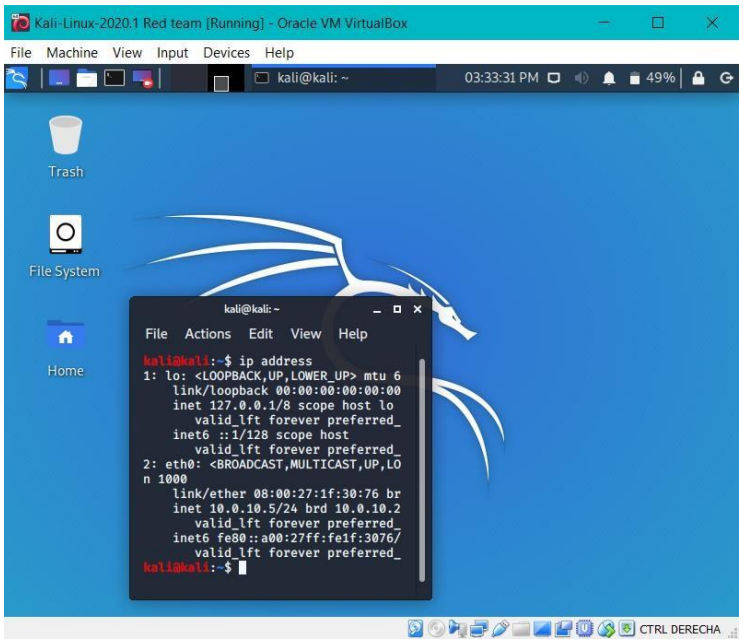


Figura 17. Visión del escritorio de la máquina de prueba de Windows 10 con su IP asignada en la consola de comandos.

Se ha elegido para este proyecto la última versión de Kali Linux disponible. Para su instalación, se ha obtenido el fichero de imagen para VBox a través de la página oficial de Offense Security. La versión de Kali Linux en la máquina virtual es la versión 2020.1

2.4.6 Cisco packet tracer (Cancelado)

Inicialmente se había pensado incluir Cisco Packet Tracer en los programas a utilizar en el proyecto, pero como se observó más tarde, no fue necesario, ya que toda la infraestructura pudo ser virtualizada directamente con VirtualBox.

El programa no ofrecía ningún tipo de ventaja frente a todos los demás instalados, por lo que se decidió no seguir adelante con su utilización en el proyecto. La versión que se suponía instalar era la que se obtiene a través de la aplicación Netacad de Cisco.

2.4.7 GNS3 (Cancelado)

Al igual que con Packet Tracer, GNS3 Iba a ser empleado como uno de los softwares a utilizar durante el proyecto, para emular los diferentes dispositivos de red necesarios. Pero de nuevo, una vez planteada la red de pruebas se comprobó que gracias al NAT directo que realiza Virtual box, no ha sido necesario incluirlo. El mismo Vbox realizar una traducción de puertos y conversión de red a modo de Router, lo cual hace descartar GNS3.

2.4.8 Confluence (Attlassian)

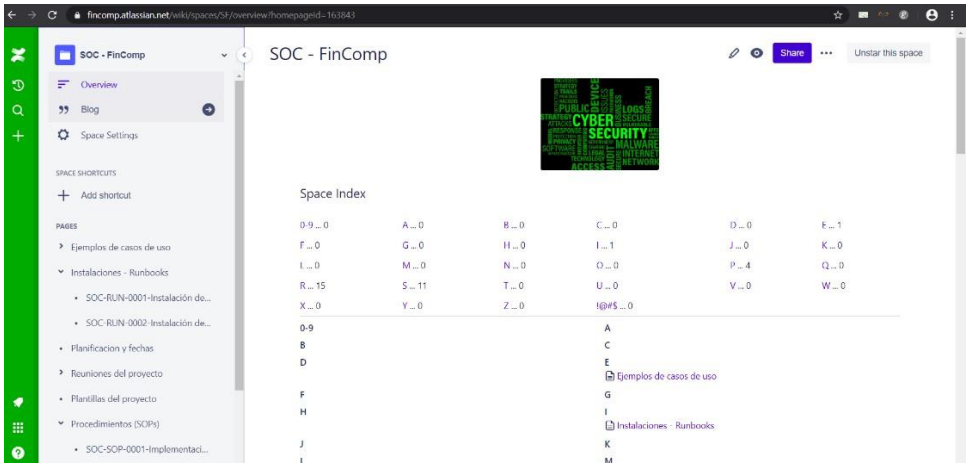


Figura 18. Página principal del SOC Fincomp de espacio creado en Confluence.

Cuando se comienza pensar en el proyecto, se observó que se necesitaría una herramienta de creación de documentación y de edición para que los miembros del SOC pudiera modificar los documentos requeridos, tanto de la parte de gestión como de las operaciones.

Una de las tareas a la hora de implementar software en la empresa es que debe cumplir con unos estándares. En este caso Conlfuence es una de las herramientas que ya se utilizan por defecto en la organización, por lo que la aprobación del software ya estaba conseguida antes. Otras opciones en este espectro de sfotware serían en propio Microsoft Teams, pero la necesidad de una licencia comercial para su uso en la red de pruebas decantó la balanza hacia el lado de Confluence en este sentido.

La herramienta debe poder dar acceso multiple y al mismo tiempo a todos los miembros, además de poder expotar los documentos facilmente. Por todo los descrito, se ha optado por la utilización de Confluence.

La herramienta es muy intuitiva, con un formato similar a las Wiki, pero a su vez se puede enriquecer con multiples añadidos, como la conexión directa con Trello o Jira.

En el caso del proyecto, se ha utilizado la versión de prueba para crear la documentación, pero existe una versióm completa para empresas a la que toda la información puede ser transferida si fuera necesario.

2.4.9 Trello

En el punto en el que ya se disponía de prácticamente todas las herramientas para proceder con el proyecto, se puso de manifiesto que se necesitaría un sistema para el seguimiento y la organización del proyecto, y dado que para la asignatura de Gestión de proyectos se trabajó con Trello, se ha decidido continuar con el mismo para el presente proyecto.

Aparte de ser uno de los programas más conocidos para la gestión de tareas y equipos, posee un gran número de extensiones, entre ellas se incluyen editores para diagramas de Gantt, justo lo que se necesita para este proyecto.

La versión utilizada para la implementación del SOC es la versión gratuita disponible en su pagina web. Existe una versión PRO para incluir múltiples usuarios y equipos, pero en el contexto del proyecto que nos concierne con la versión gratuita es suficiente.

2.4.10 Elegantt (Extensión para Trello)

Una de las razones que se ha dado para la elección de Trello como programa para la gestión del proyecto, es la posibilidad de insertar diagramas de Gantt por medio de aplicaciones externas. En el caso que nos concierne la herramienta que se ha elegido para realizar este propósito ha sido Elegantt.

El plugin es accesible directamente desde Trello una vez instalado. La versión de prueba ya permite la creación de diagramas de Gantt a partir de las tarjetas de Trello, sin necesidad de tener que insertar los datos manualmente, permite crear dependencias entre ellas y la asignación por etiquetas.

El problema con este software es su licencia, ya que la versión gratuita no permite la exportación del diagrama. Se ha optado en este caso por adquirir la licencia de pago (7 euros al mes) para poder usar esta característica. La instalación y compra del producto se realiza a través de su página web

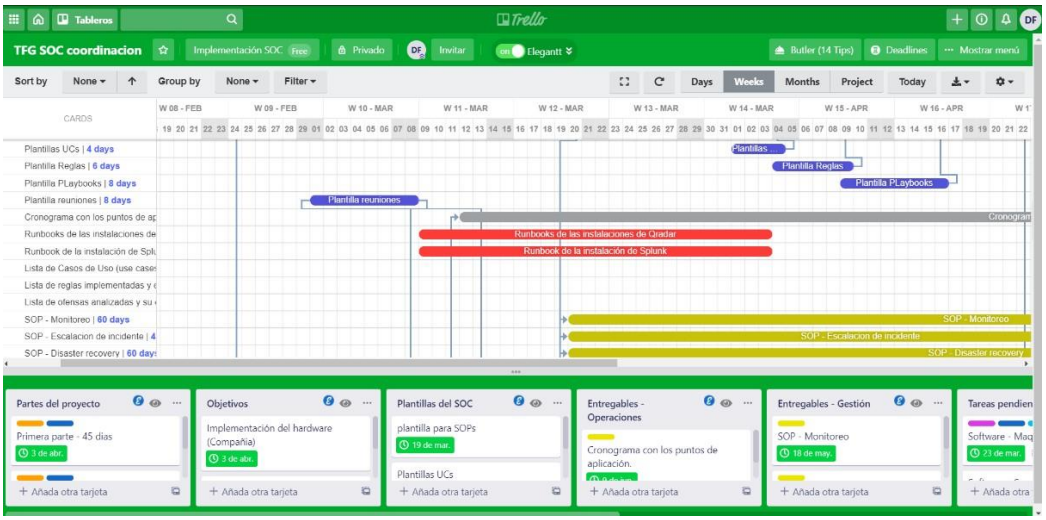


Figura 19. Ejemplo de la integración de Elegantt con Trello mediante la extensión de éste en Google Chrome.

2.5 Implementación del software

En este capítulo se va a indicar de manera breve como se han instalado todos los programas necesarios de software para poder ser usados. Muchas de las instalaciones que se mencionan serán aplicadas, bien para la zona de la red de pruebas, o para la zona de la red de la empresa; se hará una indicación en cada caso de lo que se pretende instalar. Los detalles para su configuración en cada una de las redes los dejaremos para los capítulos siguientes.

Para el software cancelado no se procederá con ninguna explicación, ya que se ha considerado innecesario para el proyecto, aunque se han llevado a cabo las instalaciones.

2.5.1 Qradar y Splunk (red empresa)

Instalación de Qradar

Acorde a la organización del proyecto esta tarea está destinada al equipo de ingeniería del SOC.

La instalación de la consola se realiza mediante conexión SSH al terminal de consola localizado en la zona SOC de la red de empresa (véase diagrama de red – Figura 22- en el capítulo 2.7). La instalación se ejecuta directamente mediante línea de comandos, para llamar al configurador de red y asignarle la IP y el host que la consola utilizará; una vez hecho, se ejecuta el comando de instalación y el sistema instala el software en el hardware de consola. Pasados unos minutos el software se instala y la aplicación es accesible mediante la IP o dominio proporcionado durante la instalación. Los procesadores de eventos son vistos como una única unidad lógica (una única IP asignada para todo), por lo que la instalación es transparente para el usuario.

Se podría considerar como finalizado el proceso, a partir de este momento se tendrían que configurar los colectores en cada zona para enviar los eventos a la consola central y a los procesadores de eventos, pero la consola ya está accesible para ser utilizada.

Instalación de Splunk

El caso es completamente similar al descrito para Qradar, simplemente el hardware cambia y las interfaces son ligeramente distintas, pero el proceso es el mismo.

Una vez los ingenieros se conectan por SSH, la instalación pide una configuración mínima de red y conectividad hacia el exterior, la cual se soluciona proporcionando IPs (no se recomiendo utilizar DHCP en este caso), dominio, DNS y Gateway. Una vez se completa la instalación, ya se puede acceder a la consola de Splunk y comenzar con su configuración.

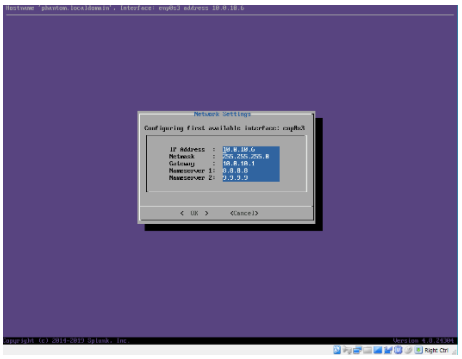


Figura 20. Parámetros de red iniciales a configurar para obtener conectividad en Splunk (mismo interfaz para todas las versiones).

2.5.2 Qradar Community Edition y Splunk Phantom (red de pruebas) (red de pruebas)

Instalación Qradar Community Edition

La instalación de Qradar Community Edition es prácticamente similar a la de la instalación de la versión completa en la empresa. La única diferencia radica en que en vez de acceder por SSH a la consola de instalación, ejecutamos la máquina virtual proporcionada por IBM, por lo que sería el equivalente a conectarnos físicamente al hardware.

Una vez proporcionadas las IP, host y DNS y Gateway se comprueba que hay conexión con Internet (ping a 8.8.8.8 por ejemplo) y se ejecuta la instalación. Después de unos 45 minutos, la consola es accesible mediante la IP que se proporcionó en el proceso de configuración.

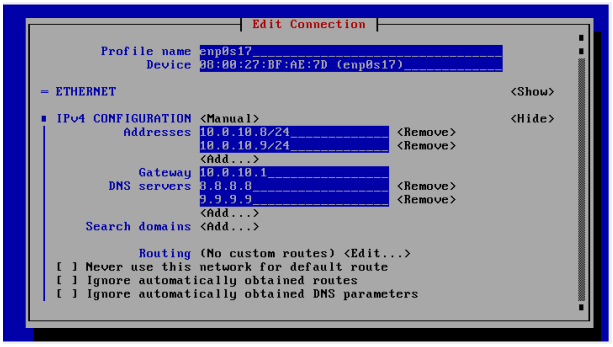


Figura 21. Interfaz gráfica de Qradar para la configuración d ellos parámetros de red. Similar a la interfaz de la versión completa.

Instalación de Splunk Phantom

Para Splunk Phantom, al ser una edición académica, es incluso más fácil, ya que la imagen que se proporciona desde la página oficial viene con la instalación finalizada, por lo que el único paso que se requiere es el de configurar la red para obtener conectividad con los demás dispositivos y salida a Internet, una vez hecho esto y mantener la máquina virtual activa, tenemos acceso a la consola mediante la IP proporcionada a tal efecto.

2.5.3 Oracle VM VirtualBox Manager (Red de pruebas)

Al ser un programa que trabaja sobre Windows, debemos simplemente obtener la versión deseada y proceder a la instalación estándar mediante el asistente de Windows.

El problema viene cuando se intentan inicializar las máquinas virtuales, si estamos trabajando sobre Windows 10 (en este caso sí), obtendremos un error de emulación. Esto viene originado por la incompatibilidad entre el motor de emulación que Windows trae por defecto (Hyper-V) y el de Virtual Box. Este error se soluciona accediendo a la BIOS del ordenador y desactivando la emulación Hyper-V. Lo que nos permite poder ejecutar las máquinas virtuales de forma correcta.

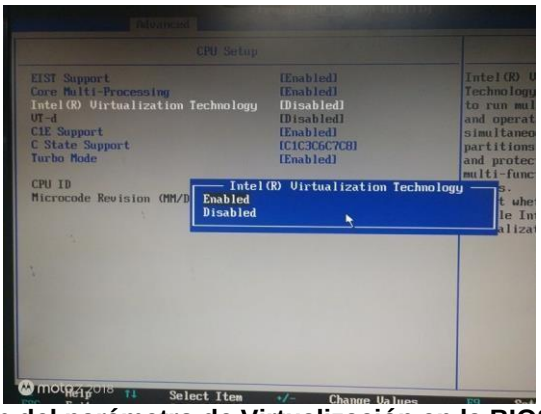


Figura 22. Modificación del parámetro de Virtualización en la BIOS de sistemas Lenovo. Imagen obtenida de Lenovo Community.

La configuración de VirtualBox será la que nos ayude a obtener comunicación de las máquinas con internet y entre ellas (importante para la monitorización de logs), pero eso lo desgranaremos en profundidad en la sección de la **configuración de la red de pruebas.**

2.5.4 Máquina Virtual Windows Pruebas

La instalación es sencilla, la máquina virtual obtenida de la página de Microsoft nos permite ejecutar directamente la máquina, sin necesidad de ninguna instalación, debemos simplemente asignarle unos valores de memoria, procesador y video decentes para poder ejecutarla. La máquina viene con un usuario administrador por defecto y una contraseña para poder acceder proporcionada por Microsoft.

2.5.5 Máquina Virtual Kali Linux – Red team

Similar al caso de Windows, si optamos por obtener la máquina virtual para Vbox directamente, no tendremos que ejecutar ninguna instalación, simplemente asignar recursos a la máquina para que funcione y la podremos ejecutar.

2.5.6 Confluence

Nuestra instalación de Confluence se realizará enteramente Online, ya que utilizaremos los recursos que éste nos proporciona sin necesidad de tener que instalar nuestro propio servidor para almacenar los datos. Este paso podría ser implementado en el futuro, pero debido al tiempo y recursos disponibles, queda fuera del alcance de este proyecto.

Para utilizar Confluence, simplemente requeriremos de una cuenta en Atlassian (compañía matriz bajo la que opera Confluence) y configurar el espacio y la compañía de la que deseamos incluir información (en este caso FinComp).

2.5.7 Trello y Elegantt

Utilizando la misma cuenta de usuario que hemos utilizado para Confluence, podremos tener acceso a Trello y Elegantt, una vez creada la cuenta, simplemente debemos acceder a la web, autenticarnos y comenzar con la configuración.

2.6 Planteamiento de la red de pruebas y configuración

Esta sección explicará el concepto de red de pruebas que se ha diseñado, cómo se ha implementado y cómo se ha configurado y probado.

2.6.1 Diseño de la red y limitaciones

De forma inicial, vamos a incluir el diagrama de red que se ha creado, para ir explicándolo sección a sección.

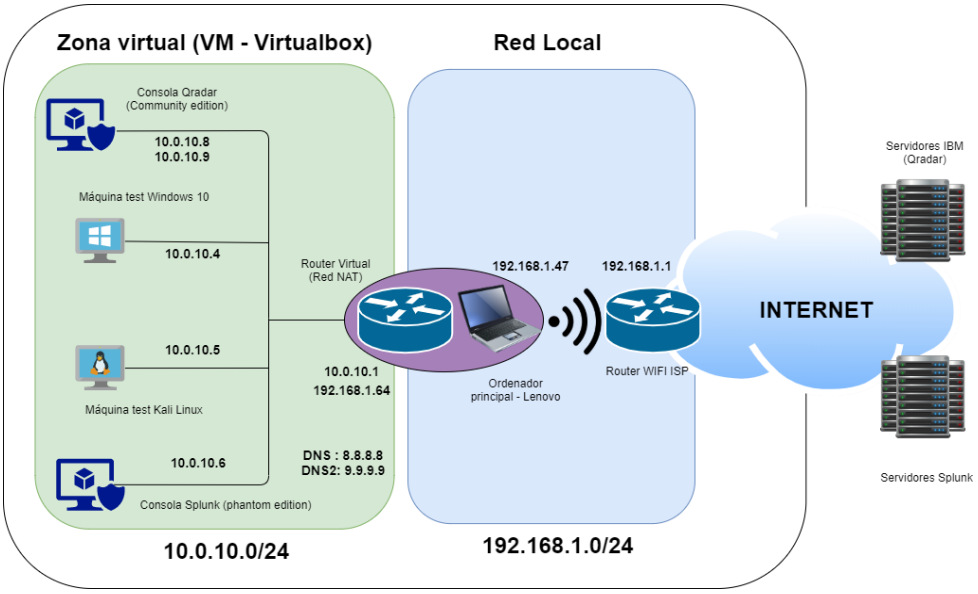


Figura 23. Diagrama de la red de pruebas creado para las pruebas de red con las soluciones SIEM.

Red Local (192.168.1.0/24)

- **Elementos de la red**

Esta red comprende el entorno de red del domicilio, es la red donde está conectado el Ordenador portátil en el que se desarrolla la parte práctica del proyecto. Este ordenador posee una IP estática asignada como 192.168.1.47. Se utiliza como enlace para el acceso a las consolas de Qradar y Splunk, mediante uso de NAT y Port Forwarding. Desde aquí se gestionan todas las configuraciones de los SIEM, así como de Virtual Box y las máquinas virtuales.

La red tiene como salida a Internet un Router del proveedor de Internet que actúa de Gateway, con la IP 192.168.1.1. Los puertos de salida están cerrados excepto para conexiones a través de los puertos 443 y 80. No se ha realizado ninguna modificación a este respecto, ya que no es necesario para mantener la conectividad con los SIEM (la conexión funciona a través de HTTPs).

Aparte de otros dispositivos conectados a la red mediante este segmento, tenemos una IP muy relevante, que es 192.168.1.64. Esta IP es la asignada por Virtual Box para realizar la NAT y enviar tráfico al exterior, traduciendo la IP de clase A en la clase C utilizada.

- **Limitaciones**

Al disponer nuestras licencias SIEM de un número limitado de colectores (uno local para ser más exactos), este dispositivo no podrá ser monitorizado, ya que se encuentra en una red distinta. No supone un impedimento muy grande, ya que al tener en la red virtual una máquina Windows, podremos cubrir ese tipo de casos de uso y alertas utilizando el colector local.

No obstante, se observan llegar eventos al SIEM con la IP de nuestro ordenador, ya que, al realizar el acceso a la consola a través de éste, los eventos que muestran información del sistema vienen asignados con su IP.

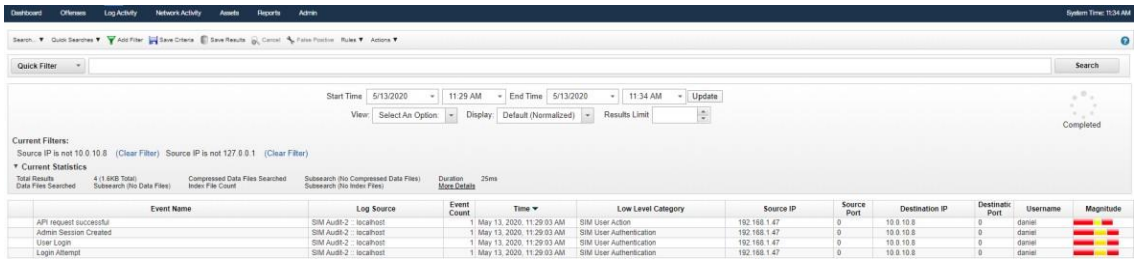


Figura 24. Referencia a la IP local (192.168.1.47) en los logs de Qradar (logins en la aplicación).

Zona Virtual (10.0.10.0/24)

- **Elementos de la red**

a) VirtualBox (10.0.10.1)

La aplicación es el eje central de funcionamiento de la red, ya que es creada directamente en el programa. Una vez que se crea la red virtual, VBox se asigna directamente la primera IP de la red para realizar el NAT al exterior.

Esta IP es la utilizada como Gateway por todos los elementos de la zona Virtual. Se han configurado como DNS los que Google facilita de forma gratuita (8.8.8.8 y 9.9.9), estos serán los utilizados por todos los elementos de red.

b) Máquina Windows (10.0.10.4)

La IP asignada a la máquina Windows se ha realizado de forma estática, para así poder tener una referencia fija a la hora de enviar los logs a las soluciones SIEM.

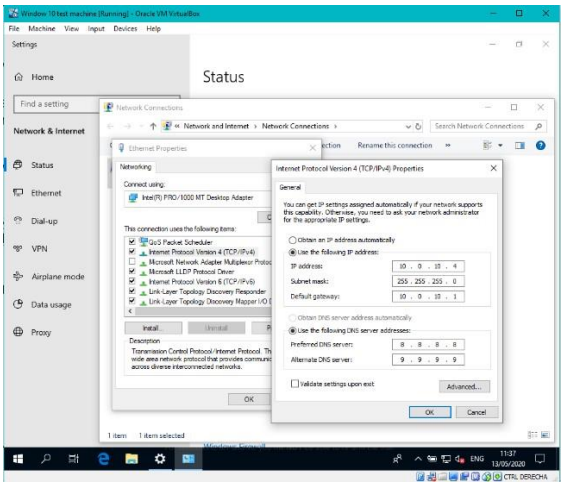


Figura 25. Asignación manual de la IP en la maquina Windows.

c) Máquina Kali Linux (10.0.10.5)

Para Kali se ha optado por la asignación de la siguiente IP disponible, la configuración de red se ha realizado de nuevo de forma manual, no forzando la asignación mediante DHCP, para asegurar que se mantiene la misma IP

d) Splunk Phantom (10.0.10.6)

Splunk Phantom ocupe la asignación de IP siguiente, dejando la siguiente IP (10.0.10.7) disponible en caso de necesidad de configuración, pero Splunk solo necesita de una dirección en lugar de dos. Se ha creado una redirección de puertos para acceder a la consola directamente desde el ordenador, sin tener que utilizar las máquinas virtuales. Tiene conexión directa con los servidores de Splunk vía Internet a través de Virtual Box.

e) Qradar Community Edition (10.0.10.8 – 10.0.10.9)

Qradar nos proporciona la posibilidad de asignar dos IPs distintas para acceder al SIEM, se han asignado dos IPs consecutivas, aunque se ha realizado la redirección de puertos solamente para la IP 10.0.10.8, ya que la segunda IP se utiliza en caso de que la primera no sea accesible, pero es totalmente funcional desde las máquinas virtuales.

Se han configurador servidores NTP para obtener una sincronización correcta con los eventos enviados directamente desde el resto de las máquinas virtuales, se han utilizado los 4 servidores NTP localizados en Bélgica, ya que es desde donde se realiza el proyecto.

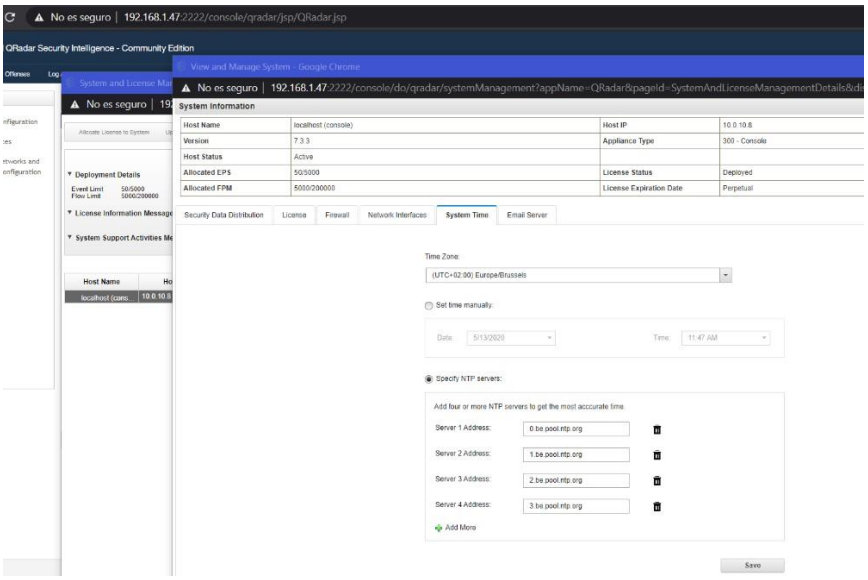


Figura 26. Asignación de los servidores NTP para sincronización de tiempo en Qradar.

- **Limitaciones y problemas**

En este caso todas las máquinas tienen conexión a Internet y se pueden comunicar entre sí. Pero de forma inicial esto no era posible, se tuvieron que abrir servicios, cambiar puertos y modificar políticas de conexión en los dispositivos, ya que para el usuario medio que utiliza este tipo de máquinas, es mejor no dejarlas abiertas por defecto.

Inicialmente se había pensado en crear las máquinas en zonas distintas de red, pero debido a la limitación en los SIEM del uso de colectores mencionado anteriormente, se tuvo que optar por incluir toda la infraestructura bajo el mismo rango de IPs.

2.6.2 Configuración de Virtual Box para conectividad

A partir de insertar todos los elementos en la red de pruebas, se observó que se necesitaría comunicarlos entre sí. El problema radica en que VBox por defecto asigna redes distintas entre los dispositivos, por lo que los dispositivos por defecto no se ven entre sí, se necesita configurar la conexión de red para que actúen todos dentro de la misma.

Para solucionar este problema, se tiene que crear una red específica dentro de VBox para asignársela a las máquinas virtuales que queramos incluir. Se puede crear una red directamente en las preferencias de la aplicación, donde asignamos el rango de red, su nombre, si queremos incluir DHCP (en nuestro caso no) o incluso asignar IPv6 en vez de IPv4.

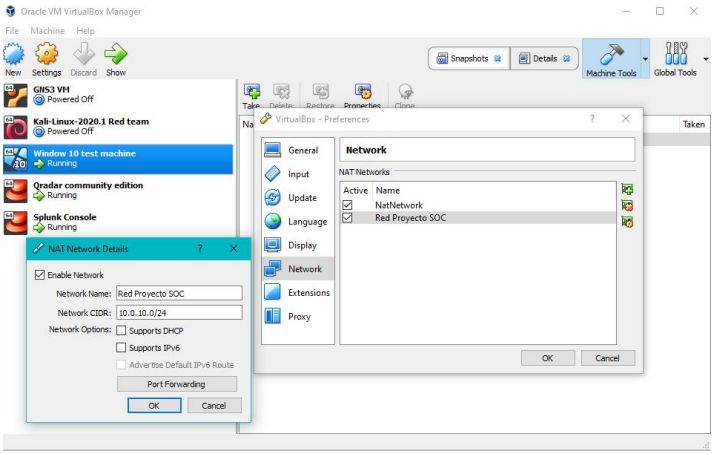


Figura 27. Creación de la red en VBox para utilizar en las máquinas virtuales.

A partir de la creación de la red, simplemente debemos asignársela a cada máquina virtual de la red, utilizando la configuración de red del tipo ¨Red NAT ¨ ya que queremos que se realice NAT para obtener salida a Internet. Si quisiéramos omitir la salida, se podría aislar la red del exterior, pero eso no interesa en este proyecto.

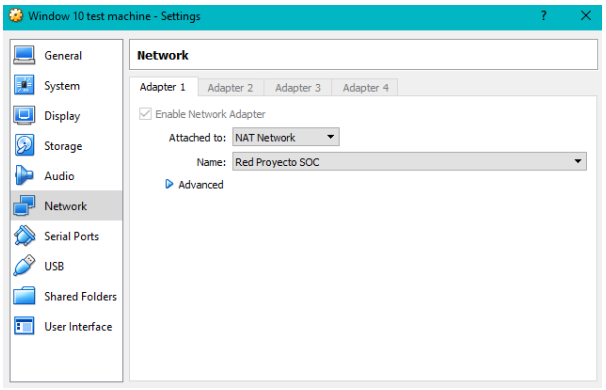


Figura 28. Asignación de la red a las máquinas virtuales.

Después de realizar esta configuración, en teoría ya se podrán realizar comunicaciones entre las máquinas virtuales.

Para finalizar la configuración de VBox, solo nos faltará tener que configurar el acceso a las consolas SIEM desde nuestro ordenador, para tener que evitar utilizar las máquinas de la red (son más lentas y resulta más tedioso).

Para poder acceder debemos realizar una redirección de puertos, enviando la conexión 443 que se realiza para acceder a los SIEM a través de un puerto de nuestro ordenador. Se utilizan los puertos 2222 y 2223 para acceder a Qradar y Splunk respectivamente. De esta forma, accediendo a nuestra IP local con el puerto especifico, podemos acceder a las consolas.

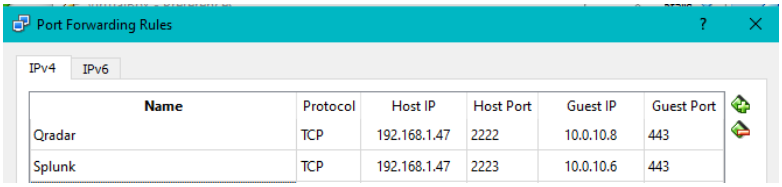


Figura 29. Redirección de puertos para los SIEM en VirtualBox.

2.7 Planteamiento de la red en la empresa

Este capítulo cubrirá el diseño que la empresa Fincomp posee dentro de su red de comunicaciones. Se ha realizado un diseño pensando en el tipo de servicio que Fincomp ofrece, intentando englobar todos los posibles elementos que una red real de empresa puede tener.

Algunas conexiones a bajo nivel se han obviado, como puede ser la zona de comunicación, donde están situados los routers (aunque se le ha asignado un rango de IPs – 10.10.0.0/22), o la zona de administradores, donde normalmente se incluyen los accesos o servidores que permiten cambiar las configuraciones de toda la red

Se ha intentado realizar un ejercicio de división en subredes, pero al no tener certeza absoluta del número de dispositivos que se van a emplear, se ha optado por no reducir el número de host por red de manera muy precisa.

En esta red no se van a incluir los pasos de configuración, ya que se asume que esta tarea ha sido llevada a cabo por la propia compañía, y no es nuestra tarea el implementar ningún elemento de red (aparte de la infraestructura SIEM), pero describiremos las diferentes zonas, y seguidamente, como se va a proceder a la monitorización de cada una de ellas.

2.7.1 Diseño de la red de empresa

Red Preproducción o Test (10.0.64.0/24)

Es la red de la empresa donde se ejecutan las pruebas de los dispositivos los cuales serán implementados en producción después de verificar su correcto funcionamiento. En esta red las políticas de seguridad están más relajadas, ya que se pueden ejecutar instalaciones, modificaciones en los sistemas y cambios en los grupos de seguridad.

Esta zona también es utilizada por el departamento de desarrollo para realizar su trabajo de creación y depuración de código, para el cual se necesitan modificaciones de librerías de código, estos cambios producirían múltiples alertas en caso de ser implementadas en producción (además de no ser acorde con las buenas prácticas).

Red Producción - Core (10.0.0.0/18)

Es la red principal de Fincomp, en esta zona encontramos todos los distintos servidores que proveen de servicios y conexión a toda la empresa. Si en esta zona existiera un incidente de seguridad tendría un gran impacto negativo en la organización.

Los accesos y politicas de seguridad están altamente restrigidos, y sólo administradores de red pueden acceder a esta sección. Todos los firewall y dispositivos de seguridad se encuentran en un estado de alta disponibilidad en estado activo-activo y duplicados a su vez, para evitar que el sistema se quede sin seguridad. En caso de caida de la red, un equipo monitoriza las 24 horas para reaccionar lo antes posible y reestablecer el servicio.

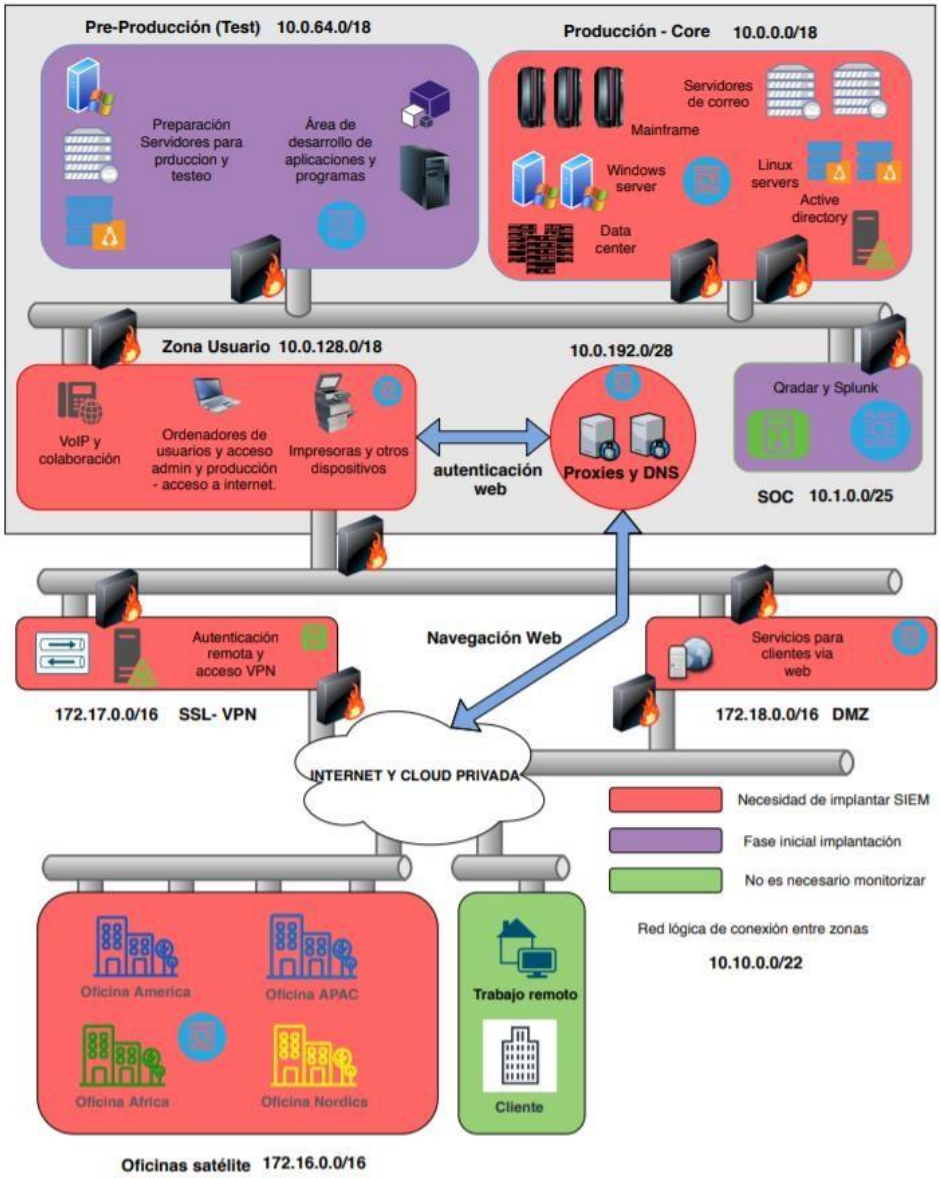


Figura 30. Diagrama de red de Fincomp creado para el proyecto.

Zona usuario (10.0.128.0/18)

La zona de usuario es básicamente la zona donde los empleados de Fincomp se conectan. Los dispositivos de trabajo, impresoras, sistemas de voz IP, teleconferencia o presentación están localizados aquí. Casos especiales de posibles movimientos laterales se deben crear, ya que es uno de ellos puntos de entrada vulnerables, ya sea por un empleado actuando de manera fraudulenta, o introduciendo a través de phishing o malware acceso de actores externos a la red.

Zona SOC (10.1.0.0/25)

La zona SOC se ha creado específicamente para este proyecto. Aquí se incluyen todas las aplicaciones relacionadas con la monitorización y respuesta ante amenazas. A parte de los SIEM, las soluciones antivirus, proxy inverso, Email security están aquí

implementadas. En este rango de IP estarán localizadas las consolas de Qradar y Splunk en Fincomp.

Red Proxy/DNS (10.0.192.0/28)

La red proxy es una red intermedia a la que se conectan los empleados de la empresa para acceder fuera de Fincomp, todo el tráfico proxy y DNS pasa a través de esta red.

Casos especiales de posible elusión de esa red podrían ser implementados. Aquí se podrían observar los primeros indicios de conexiones a páginas maliciosas o comprobaciones de que no se envían a Internet material confidencial de la empresa.

Red SSL-VPN (172.17.0.0/16)

Esta red es la red que enruta el acceso de los empleados mediante la VPN, si bien trabajan en otra localización o desde casa. También es el punto de conexión con el resto de las delegaciones de Fincomp, compartiendo archivos mediante VPN.

Los firewalls con capacidad SSLVPN se encuentran en este segmento de la red. Casos interesantes para esta res serían el monitorizar intentos fallidos de conexión mediante usuario, lo que podría indicar un intento de ataque de fuerza bruta desde el exterior.

Red DMZ (172.18.0.0/16)

Es la red de cara a Internet de la empresa, donde se aloja la web principal de esta y otros servicios para clientes. En esta parte se produciría el NAT entre los servidores públicos de la empresa y los privados. Posibles intentos de DDoS o escáneres podrían ser vistos en esta red.

Red oficinas satélite (172.16.0.0/16)

Este rango comprende las IPs de los dispositivos conectados en cada una de las delegaciones de la empresa, la forma de monitorizar esta VLAN sería la misma que la zona usuario descrita más arriba en el capítulo.

2.7.2 Proceso de inclusión de zonas dentro de la monitorización

Este proyecto cubrirá principalmente al inicio la inclusión de los SIEM en la red de Preproducción, con los casos de uso aplicados de forma general en todas las zonas. Se irán incluyendo los eventos paulatinamente del resto de zonas de la red, para finalizar en la monitorización de la red de producción si todo funciona correctamente.

En caso de que no se puedan incluir todas las zonas y probar sus casos de uso correctamente de forma previa, producción no será incluida.

2.8 Plan de recuperación ante desastres (disaster recovery)

Para empresas como Fincomp, uno de los objetivos esenciales es el mantenimiento del servicio de forma activa las 24 horas del día. Nadie se imaginaría el no poder acceder al servicio de banca en horario nocturno o los fines de semana.

Por ello, uno de los requerimientos en el proyecto es el diseño es la creación de un plan de respuesta antes desastres u otras contingencias que pudieran ocasionar una disrupción en el servicio que la empresa ofrece.

En este caso, se ha creado un procedimiento completo en la aplicación Confluence, el documento de denomina *SOC-SOP-0005-Plan de recuperación ante desastres (Disaster Recovery).* Este procedimiento o Security Operation Procedure (SOP). El documento se encuentra incluido en la sección de los anexos (Sección 6.3), para ser consultado.

Este documento incluye el sistema en el que los dispositivos serán implementados para maximizar la disponibilidad, así como inclusión de reglas de monitorización en caso de que alguno de los dispositivos se encuentre inaccesible.

2.9 Creación del acceso granular para los miembros del SOC

Una de las tareas de los ingenieros del SOC es el mantener y gestionar la base de datos de usuarios que requieren acceso a las herramientas SIEM. En este caso, los accesos a usuarios se realizan de forma distinta en cada uno de los SIEM, se van a explicar ambos casos, otorgando las mismas cuentas y accesos en ambos para todos los miembros del SOC

2.9.1 creación de accesos en Qradar

Qradar estructura su acceso granular en tres fases.

- **Creación del perfil de seguridad:** Este primer paso permite crear niveles de acceso a los eventos recogidos en el SIEM. Se han creado tres perfiles de seguridad:

    1. Perfil de Analista
    2. Perfil de Ingeniero
    3. Perfil de Gestión

- **Creaciones de rol de usuarios:** El segundo paso es otorgar a cada grupo de usuarios el tipo de permisos con los que pueden ejecutar acciones en el SIEM

    1. Rol de Analista
    2. Rol de Ingeniero
    3. Rol de Gestión

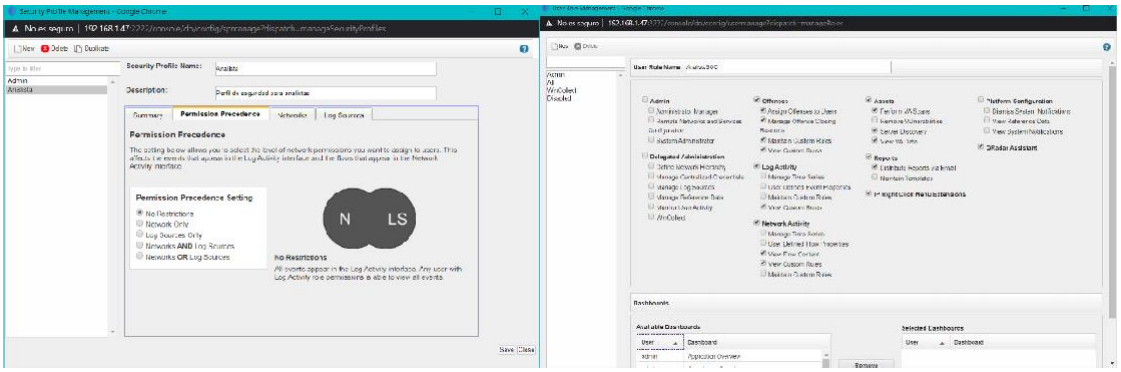


Figura 31. Ejemplo creación de un perfil y de un rol de analista.

- Creación de las cuentas de usuario: Con los dos pasos anteriores completados, simplemente faltaría crear todas las cuentas de usuario, asignándoles el rol y el perfil de seguridad correspondiente.

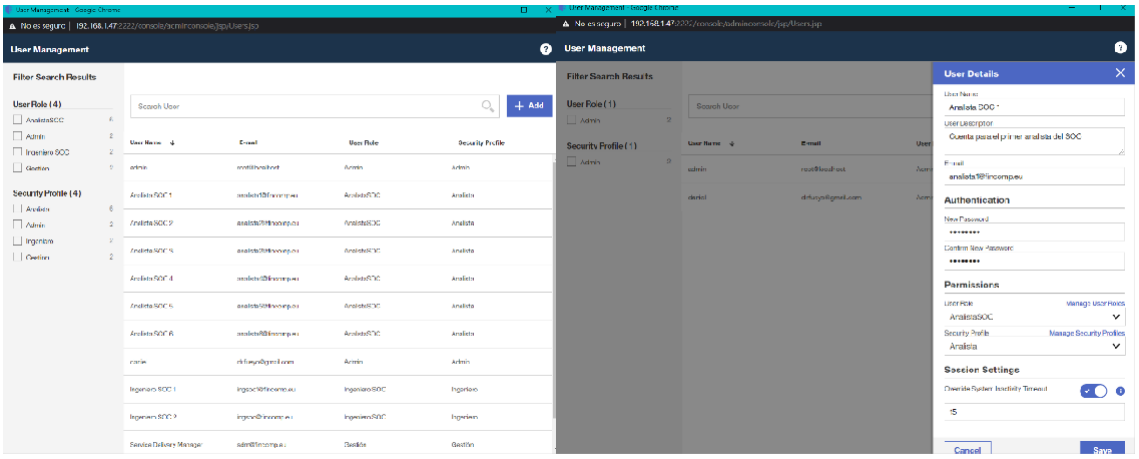


Figura 32. Creación de las cuentas para los usuarios del SOC.

2.9.2 creación de accesos en Splunk

En la herramienta Splunk, en lugar de realizar la política de autenticación por usuario se ha optado por una política general para todos por igual, pudiendo incluir dos niveles de autenticación si fuera necesario. Esta modificación es el primer paso para configurar el acceso granular. Se han puesto parámetros específicos para crear las contraseñas, así como el tiempo de inactividad.

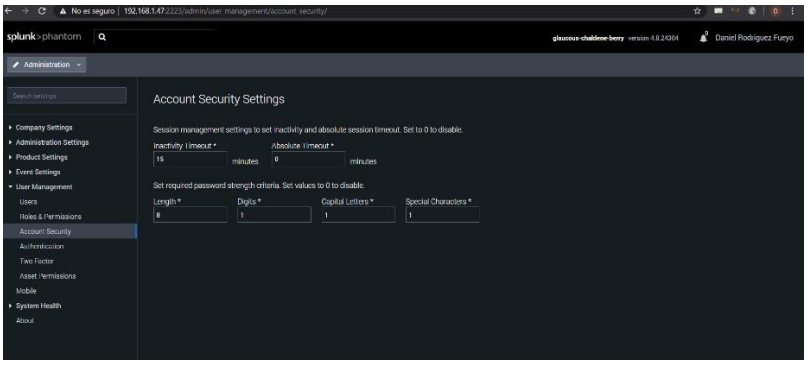


Figura 33. Configuración elegida para los parámetros de acceso de las cuentas.

Una vez que los parámetros son los que se desea, se deben crear los roles y permisos específicos para cada puesto, se ha procedido de nuevo con tres permisos y roles distintos:

- Rol ingenieros
- Rol analistas
- Rol gestión

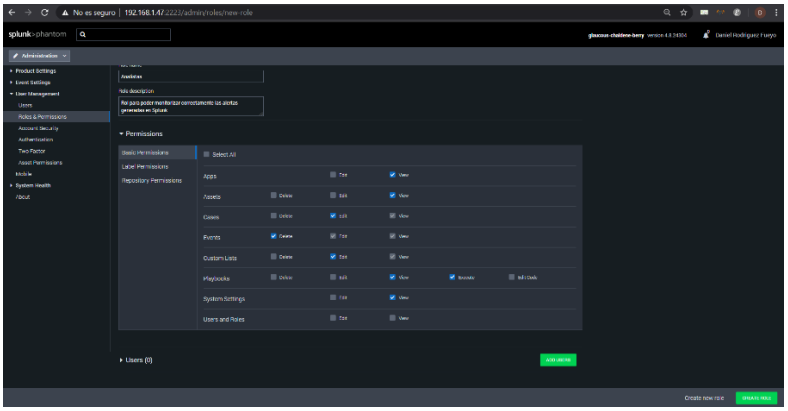


Figura 34. Ejemplo de la creación de un rol en Splunk.

El paso final es la creación de todas las cuentas necesarias, para poder ser utilizadas en Splunk. Se facilita un email asignado a cada una, con el que los usuarios podrán cambiar la contraseña si fuera necesario.

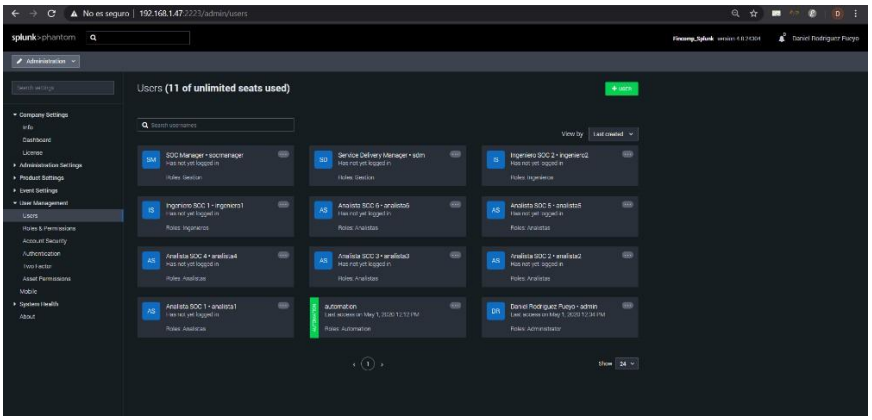


Figura 35. Muestra de las cuentas de usuario creadas en Splunk.

2.10 Plan de entrenamiento para nuevos analistas

Para que el SOC pueda funcionar de forma autónoma y una vez que el proyecto finalice, debe ser implementado un proceso de entrenamiento para nuevos analistas, e introducir a los nuevos empleados a los procesos de funcionamiento del SOC.

Como este documento puede ser requerido, se ha incluido como uno de los procedimientos básicos del SOC, creando la documentación en la herramienta Confluence. El documento se denomina *SOC-SOP-0003-Entrenamiento para analistas.* Este documento se encuentra en la sección de anexos (sección 6.7), con los pasos básicos para organizar un entrenamiento de analistas correcto en tiempo y forma.

2.11 Inclusión de los registros en las herramientas SIEM (log onboarding)

A partir de tener la documentación del SOC, la red de pruebas y de empresa, se puede proceder con la parte más interesante del proyecto, y es hacer funcionar correctamente los SIEM, insertando los eventos de otros dispositivos, crear alertas relacionadas y analizarlas para responder ante ellas.

El primer paso de toda esta sección final es la de incluir los eventos generados por otros sistemas, para ser interpretados. Se van a incluir los eventos de dos máquinas virtuales distintas, una es la VM de Windows 10, mientras que la otra es la máquina de pruebas Kali Linux.

2.11.1 Inclusión de los logs en Qradar

Eventos recibidos desde un sistema Windows

Para comenzar, no debemos realizar grandes cambios de configuración directamente en Qradar; para recibir los logs de un sistema Windows, debemos realizar los cambios de configuración en la propia máquina Windows.

El primer paso es la instalación de Wincollect en la máquina virtual. Para ello se puede obtener el instalador en la página de IBM fix central. Se debe instalar la versión acorde al sistema operativo (en nuestro caso 64 bits) y el parche parta la versión correspondiente. En la instalación se nos pide a dónde enviar los eventos, seleccionamos la IP de Qradar (10.0.10.8) y el puerto de Syslog (514). Una vez que se termina la instalación deberían poder recibirse los eventos, pero no están activados

Una vez que se ha realizado la instalación, debemos elegir qué tipo de elementos queremos que se envíen, debe realizarse a través de las políticas de seguridad locales, éstas se encuentran dentro de las herramientas del sistema. Una vez accedidas, seleccionamos las que queremos activas, en el caso de nuestro proyecto las activaremos todas, pero se pueden elegir unas específicas (intentos de autenticación, ejecución de procesos, cambios en el registro…).

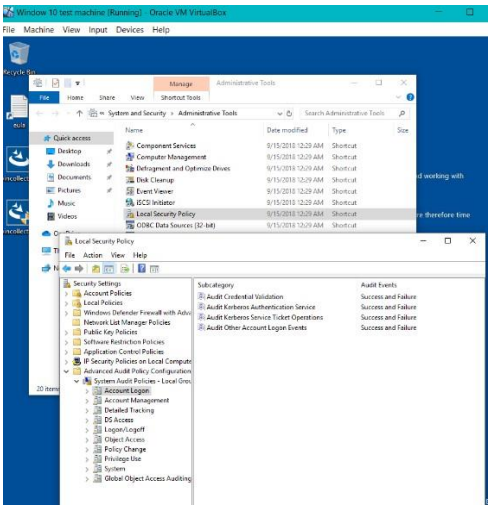


Figura 36. Acceso a las políticas de seguridad y su activación.

En este caso, si accedemos a Qradar deberíamos comenzar a ver eventos llegar, en caso de que lo hayamos configurado convenientemente. Si no se observan logs, deben revisarse si el firewall de Windows permite el envío de este tipo de logs. En nuestro caso observamos como los eventos comienzan a llegar a Qradar, y parece que el log source (el origen de los logs) se identifica como el ordenador de Windows 10, sin necesidad de hacer nada en la consola.

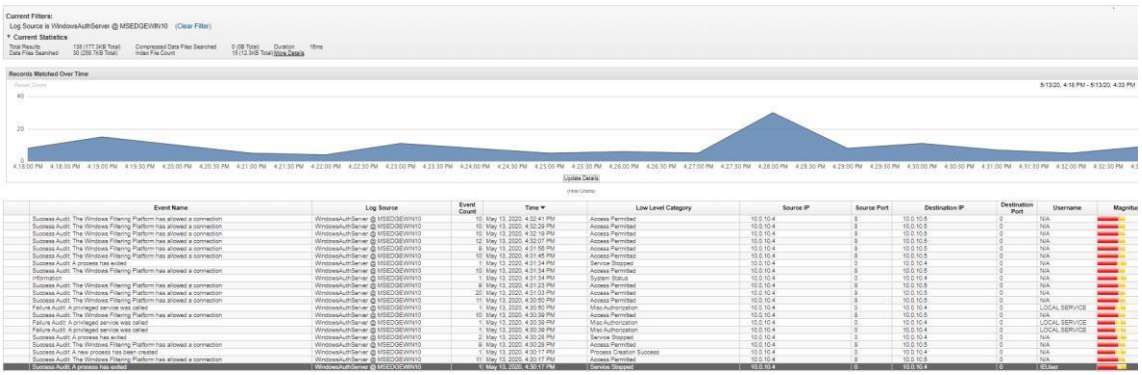
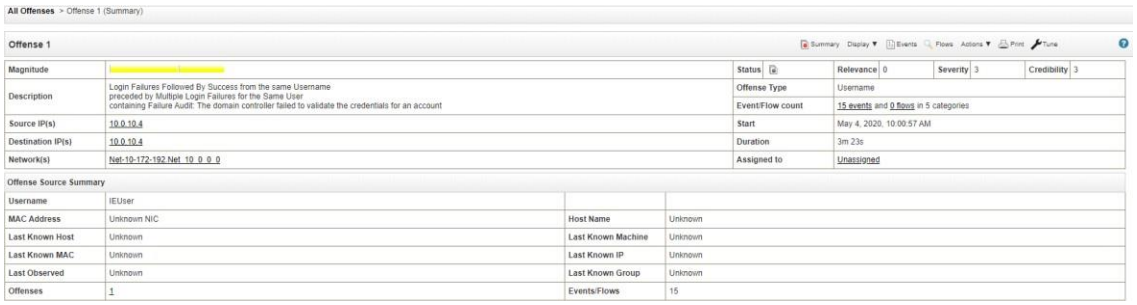


Figura 37. Ejemplo de eventos recibidos en Qradar.

En este momento hemos confirmado que los eventos llegan a la consola. Si queremos confirmar que funcionan al 100% podemos forzar que se genere una alerta por defecto, ya que Qradar incluye alertas creadas por IBM, para comenzar a monitorizar las alertas simplemente instalando el producto (out-of-the-box).

Para generar una alerta, podemos simplemente intentar entrar en la cuenta de Windows y fallar la contraseña 5 veces o más, y seguidamente poner la correcta. Qradar detectará estos eventos, los juntará en una alerta y generará una ofensa.



All Offenses > Offense 1 (Summary)

Offense 1

Summary | Display | Events | Flows | Actions | Print | Tune

Magnitude		Status		Relevance	0	Severity	3	Credibility	3
Description	Login Failures Followed By Success from the same Username preceded by Multiple Login Failures for the Same User containing Failure Audit: The domain controller failed to validate the credentials for an account	Offense Type	Username				
		Event/Flow count	15 events and 0 flows in 5 categories				
Source IP(s)	10.0.10.4	Start	May 4, 2020, 10:00:57 AM				
Destination IP(s)	10.0.10.4	Duration	3m 23s				
Network(s)	Net-10-172-192.Net_10_0_0_0	Assigned to	Unassigned				

Offense Source Summary

Username	IEUser		
MAC Address	Unknown NIC	Host Name	Unknown
Last Known Host	Unknown	Last Known Machine	Unknown
Last Known MAC	Unknown	Last Known IP	Unknown
Last Observed	Unknown	Last Known Group	Unknown
Offenses	1	Events/Flows	15

Figura 38. Ejemplo de una alerta generada por el usuario (IEUser) por fallar la contraseña múltiples veces y después acertar la correcta.

Eventos recibidos desde un sistema Linux

Si se quieren obtener eventos de máquinas con sistema operativo Linux (la distribución en este caso no es relevante, todas siguen el mismo sistema) debemos realizar cambios en la maquina Linux pero aquí también en el propio Qradar.

Para comenzar, se debe indicar a Linux que debe enviar los logs a Qradar. Para llevar a cabo esta tarea se debe modificar el archivo de Syslog de Linux (*Rsyslog.conf*) y añadir a las entradas establecidas el valor de la IP de Qradar y los tipos de logs que vamos a enviar, que son, en este caso, todos. El comando a introducir en el archivo de Syslog sería el siguiente:

- *. * @10.0.10.8:514

Esta entrada indicaría al Syslog que debe enviar todos los eventos (*.*) a la IP mencionada de Qradar por el puerto 514. Si quisiéramos, por ejemplo, enviar los eventos de autenticación podríamos especificarlos (auth. *)

Esto debería permitir obtener los logs desde Qradar, pero el problema viene en que el puerto 514 está bloqueado por defecto en Kali. Debemos utilizar el firewall para abrir los puertos.

Como Kali no viene con un Firewall por defecto, se instala uno. Se ha elegido UFW (unattended Firewall), con el activo, abrimos las comunicaciones.

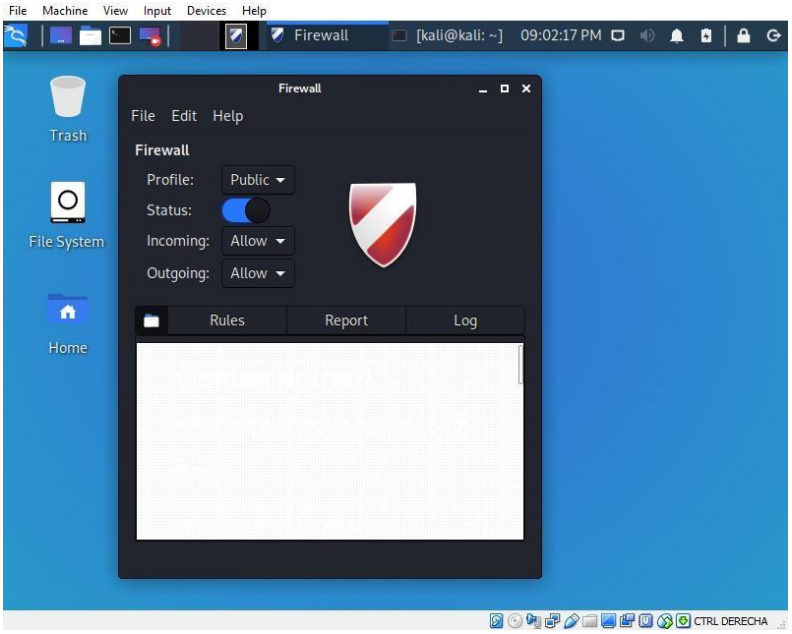


Figura 39. Firewall de Kali Linux instalado y con las comunicaciones entrada/salida abiertas.

Podemos observar como ahora llegan los eventos a Qradar. Pero el evento se marca como genérico, por lo que debemos crear un Log source en Qradar para que agregue los campos correctos a los eventos.

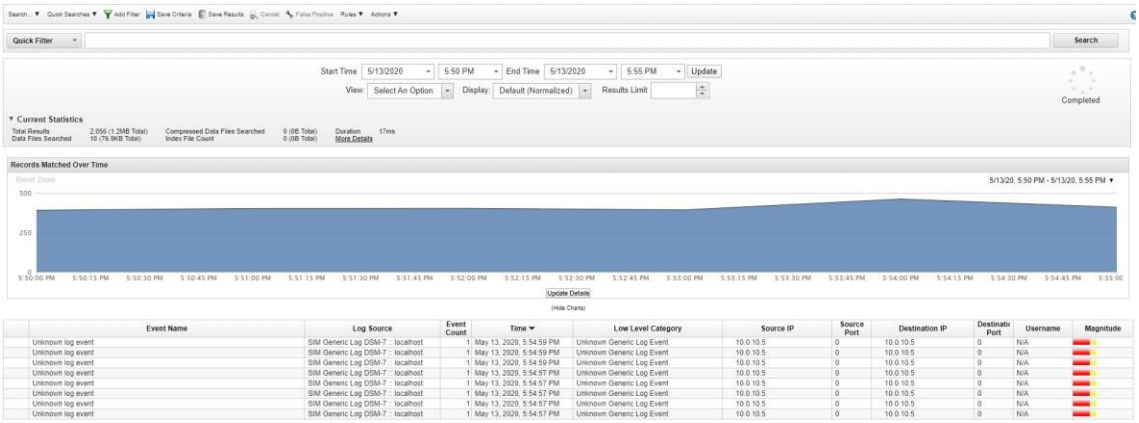


Figura 40. Eventos de Kali Linux llegan a Qradar.

Mediante la sección Log Sources en Qradar agregamos el log source para Kali Linux. Esto debería darnos los eventos específicos asignados a él.

Log Sources (11)

	ID	Name	Log Source Type	Creation Date	Last Event	Enabled	Log Source Identifier
☐	66	Anomaly Detection Engine-2 :: localhost	Anomaly Detection Engine	Apr 3, 2020 11:58 PM	May 4, 2020 8:47 PM		127.0.0.1
☐	67	Asset Profiler-2 :: localhost	Asset Profiler	Apr 3, 2020 11:58 PM	May 2, 2020 1:51 PM		127.0.0.1
☐	63	Custom Rule Engine-8 :: localhost	Custom Rule Engine	Apr 3, 2020 11:58 PM	May 14, 2020 3:36 PM		10.0.10.8
☐	69	Health Metrics-2 :: localhost	Health Metrics	Apr 3, 2020 11:58 PM	May 16, 2020 7:41 PM		127.0.0.1
☑	312	Kali Linux Red Team	Linux OS	May 13, 2020 6:15 PM	May 14, 2020 4:25 PM		kali
☐	214	LENOVO-P50-DRF	Microsoft Windows Security Event Log	May 1, 2020 4:10 PM			LENOVO-P50-DRF
☐	68	Search Results-2 :: localhost	Search Results	Apr 3, 2020 11:58 PM	May 2, 2020 11:51 AM		127.0.0.1
☐	64	SIM Audit-2 :: localhost	SIM Audit	Apr 3, 2020 11:58 PM	May 16, 2020 7:41 PM		127.0.0.1

Figura 41. Nuevo Log Source agregado con el nombre ¨Kali Linux Red Team¨.

Una vez unos 50 eventos más sean incluidos en Qradar, el log source que hemos creado debería tomar control y obtener el nombre correcto.

Event Name	Source IP (Unique Count)	Destination IP (Unique Count)	Destination Port (Unique Count)	Log Source (Unique Count)	Low Level Category (Unique Count)	Protocol (Un Count)
Linux login messages Message	10.0.10.5	10.0.10.5	0	Kali Linux Red Team	Stored	Other
Session Opened	10.0.10.5	10.0.10.5	0	Kali Linux Red Team	Auth Server Session O...	Other
PAM cron su_impersonation	10.0.10.5	10.0.10.5	0	Kali Linux Red Team	Privilege Access	Other
PAM Session Closed	10.0.10.5	10.0.10.5	0	Kali Linux Red Team	Auth Server Session C...	Other
Cron Command	10.0.10.5	10.0.10.5	0	Kali Linux Red Team	Cron Status	Other
An authentication attempt was unsuccessful	10.0.10.5	10.0.10.5	0	Kali Linux Red Team	General Authentication...	Other
Session Closed	10.0.10.5	10.0.10.5	0	Kali Linux Red Team	Auth Server Session C...	Other

Figura 42. Eventos correctos llegan con sus campos ordenador correctamente.

Como se probó con Windows, vamos a intentar fallar la contraseña unas cuantas veces y seguidamente entrar de forma correcta. Vemos como con los eventos correctamente introducidos, se genera una ofensa de forma correcta:

All Offenses > Offense 2 (Summary)

Offense 2 — Summary | Display ▼ | Events | Flows | Actions ▼ | Print | Tune

Magnitude	[redacted]	Status		Relevance 3	Severity 5	Credibility 2
Description	Login Failures Followed By Success from the same Username preceded by Multiple Login Failures for the Same User containing An authentication attempt was unsuccessful	Offense Type	Username			
		Event/Flow count	20 events and 0 flows in 4 categories			
Source IP(s)	10.0.10.5	Start	May 14, 2020, 3:38:35 PM			
Destination IP(s)	10.0.10.5	Duration	3m 18s			
Network(s)	Net-10-172-192 Net_10_0_0_0	Assigned to	Unassigned			

Offense Source Summary

Username	kali		
MAC Address	Unknown NIC	Host Name	Unknown
Last Known Host	Unknown	Last Known Machine	Unknown
Last Known MAC	Unknown	Last Known IP	Unknown
Last Observed	Unknown	Last Known Group	Unknown
Offenses	1	Events/Flows	20

Figura 43. Ejemplo de una ofensa (alerta) generada por Qradar a partir de los eventos de la maquina Kali Linux.

2.11.2 Inclusión de los logs en Splunk

Los logs en Splunk Phantom no se pueden enviar directamente en la versión Phantom de la que se dispone de forma gratuita, en el caso de la red de pruebas se van a enviar los eventos directamente que se generan en Qradar a la aplicación, así, cuando una alerta se genere en Qradar, obtendremos su equivalente en Splunk.

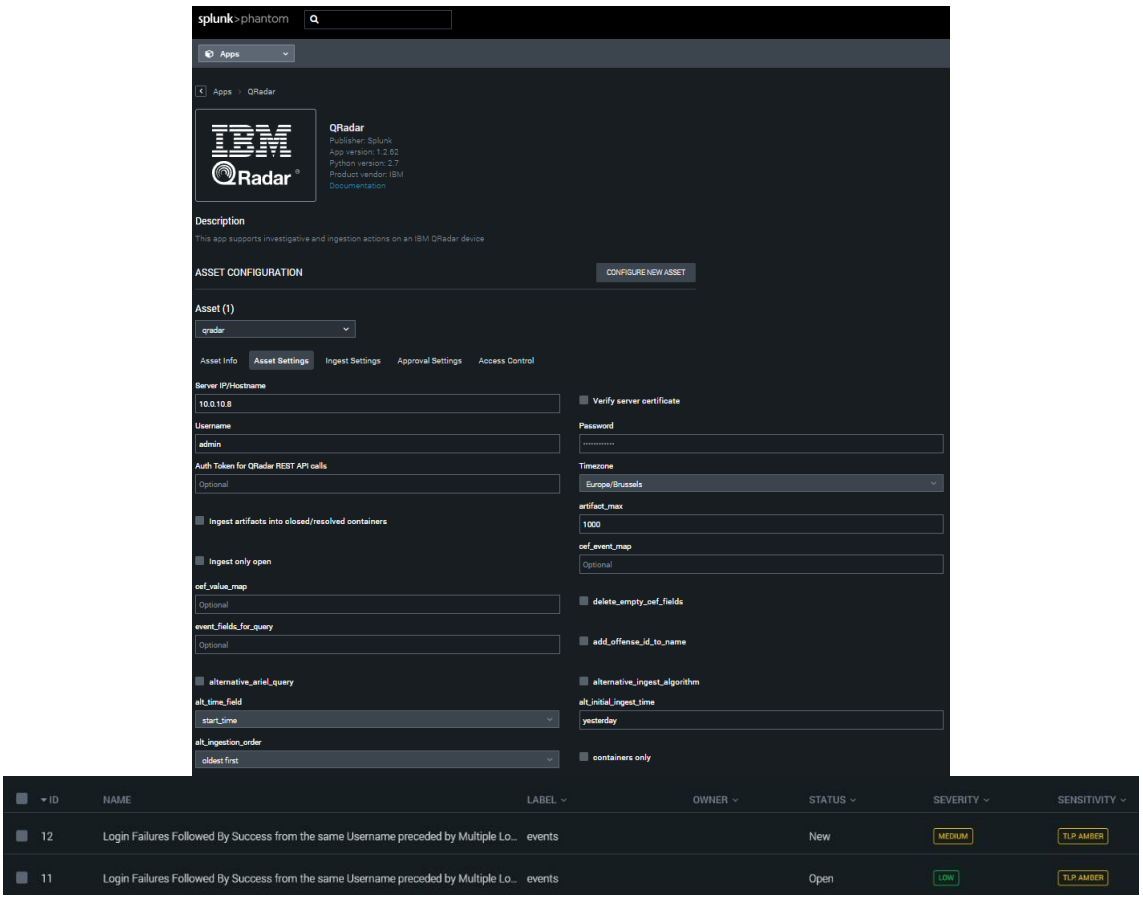


Figura 44. Inclusión de los eventos en Splunk a través de Qradar y ejemplo de las alertas enviadas.

Para la versión de empresa, el sistema de inclusión de logs sigue exactamente el mismo sistema que en Qradar.

2.12 Creación de los casos de uso (Use cases)

A partir de ese punto se deja de lado la configuración de los SIEM en sí para centrarnos en la parte de monitorización. Los SIEM viene con casos de uso y reglas predefinidas que se activan nada más instalar las consolas, como vimos en las pruebas de recepción de eventos en la sección 2.11.1 y 2.11.2. Estas reglas son perfectamente funcionales, pero tiene dos inconvenientes:

- Suelen basarse en bloques de acciones (Building blocks), los cuales son opacos para el usuario o incluso el administrador, no sabemos lo que contienen exactamente.
- Las configuraciones tienen un alcance muy general, por lo que en muchas ocasiones no monitorizan aspectos concretos que serían interesantes para la compañía que adquiere el producto.

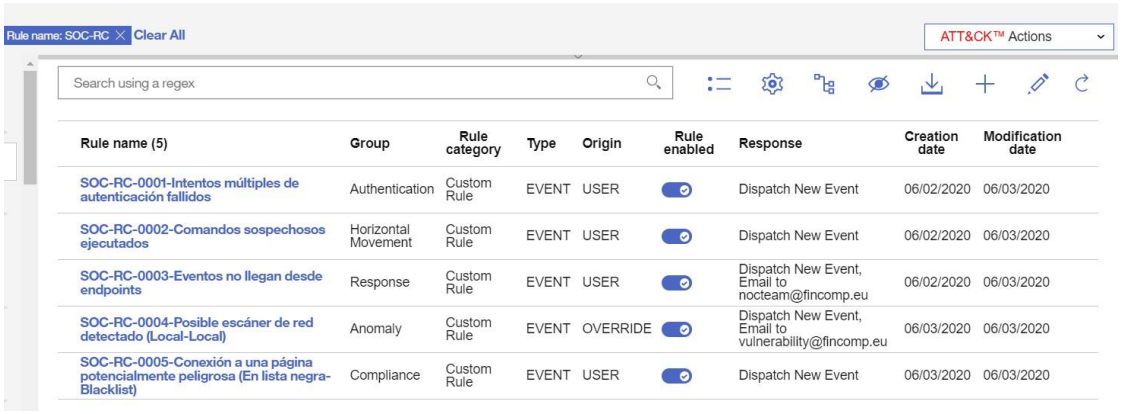
Para llevar a cabo la tarea de crear casos de uso, se ha generado un procedimiento, denominado *SOC-SOP-0001-Implementación de Casos de Uso (CU)*. Este procedimiento explica los pasos necesarios para la implementación de un caso de uso, bien por parte exclusiva del SOC, o en colaboración con otros departamentos. El procedimiento puede encontrarse en la sección 6.4, en los anexos.

2.13 Configuración de las reglas acordes a los casos de uso.

Una vez que los casos de uso han sido creados y verificados por el Service Delivery Manager, es el momento de ingeniería para comenzar con la creación y la configuración de las reglas en el SIEM.

Para ello de nuevo se ha creado la documentación necesaria para la creación del procedimiento para nuevas reglas y además 5 reglas específicas obtenidas a partir de los 5 casos de usos iniciales.

Estos documentos se encuentran en la sección 6.5 de los anexos.



Rule name (5)	Group	Rule category	Type	Origin	Rule enabled	Response	Creation date	Modification date
SOC-RC-0001-Intentos múltiples de autenticación fallidos	Authentication	Custom Rule	EVENT	USER		Dispatch New Event	06/02/2020	06/03/2020
SOC-RC-0002-Comandos sospechosos ejecutados	Horizontal Movement	Custom Rule	EVENT	USER		Dispatch New Event	06/02/2020	06/03/2020
SOC-RC-0003-Eventos no llegan desde endpoints	Response	Custom Rule	EVENT	USER		Dispatch New Event, Email to nocteam@fincomp.eu	06/02/2020	06/03/2020
SOC-RC-0004-Posible escáner de red detectado (Local-Local)	Anomaly	Custom Rule	EVENT	OVERRIDE		Dispatch New Event, Email to vulnerability@fincomp.eu	06/03/2020	06/03/2020
SOC-RC-0005-Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)	Compliance	Custom Rule	EVENT	USER		Dispatch New Event	06/03/2020	06/03/2020

Figura 45. Muestra de las reglas implementadas en el SIEM (Qradar).

2.14 Creación de los Playbooks para los analistas

Para finalizar con la creación de documentos de monitorización, se han creado 5 libros de reglas de ejemplo para el análisis de cada una de las reglas generadas en el SIEM, además del procedimiento para crear estos libros de reglas.

La documentación se puede encontrar en la sección 6.6 de los anexos.

2.15 Testeo de reglas y respuesta con casos reales

Para comprobar como el SOC funciona a nivel de monitorización y análisis, se ha realizado el ejemplo con las 5 reglas creadas en el contexto de la empresa para valorar si las acciones son efectivas o no, para así proceder a cerrar el proyecto.

All Offenses View Offenses with: Select An Option:

Current Search Parameters:

Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

Id	Description	Offense Type	Offense Source	Magnitude	Source IPs	Destinati
49	SOC-RC-0005-Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)	Destination IP	213.73.40.242		10.0.10.4	213.73.40.242
50	Success Audit: The Windows Filtering Platform has allowed a connection	Destination IP	204.236.236.127		10.0.10.4	204.236.236.1
51	Success Audit: The Windows Filtering Platform has allowed a connection	Destination IP	91.198.174.194		10.0.10.4	91.198.174.19
46	SOC-RC-0004-Posible escáner de red detectado (Local-Local)	Source IP	10.0.10.5		10.0.10.5	10.0.10.4
43	SOC-RC-0002-Comandos sospechosos ejecutados	Username	LOCAL SERVICE		10.0.10.4	10.0.10.4
42	SOC-RC-0001-Intentos múltiples de autenticación fallidos	Username	kali		10.0.10.5	10.0.10.5
45	SOC-RC-0002-Comandos sospechosos ejecutados	Username	LOCAL SERVICE		10.0.10.4	10.0.10.4
41	SOC-RC-0002-Comandos sospechosos ejecutados	Username	IEUser		10.0.10.4	10.0.10.4
48	SOC-RC-0003-Eventos no llegan desde endpoints	Log Source	Custom Rule Engine-8 :: localh...		0.0.0.0	0.0.0.0
44	Excessive Firewall Denies Between Hosts containing Failure Audit: The Windows Filtering ...	Source IP	10.0.10.5		10.0.10.5	10.0.10.4
47	Failure Audit: A privileged service was called	Username	IEUser		10.0.10.4	10.0.10.4
2	Login Failures Followed By Success from the same Username preceded by Multiple Login...	Username	kali		10.0.10.5	10.0.10.5
1	Login Failures Followed By Success from the same Username preceded by Multiple Login...	Username	IEUser		10.0.10.4	10.0.10.4

Figura 46. Vista de las alertas generadas en los SIEM

2.15.1 SOC-RC-0001-Intentos múltiples de autenticación fallido

Contexto en la empresa:

El SOC detecta que una cuenta ha estado realizando varios intentos de autenticación fallidos. En este caso se debe verificar primero en la alerta si la actividad puede ser sospechosa o no.

Event Information

Event Name	An authentication attempt was unsuccessful						
Low Level Category	General Authentication Failed						
Event Description	An authentication attempt was unsuccessful						
Magnitude	(5)	Relevance	9	Severity	3	Credibility	1
Username	kali						
Start Time	Jun 2, 2020, 6:22:36 PM	Storage Time	Jun 2, 2020, 6:22:36 PM	Log Source Time	Jun 2, 2020, 3:12:46 PM		

Figura 47. Vista de uno de los eventos de autenticación fallidos.

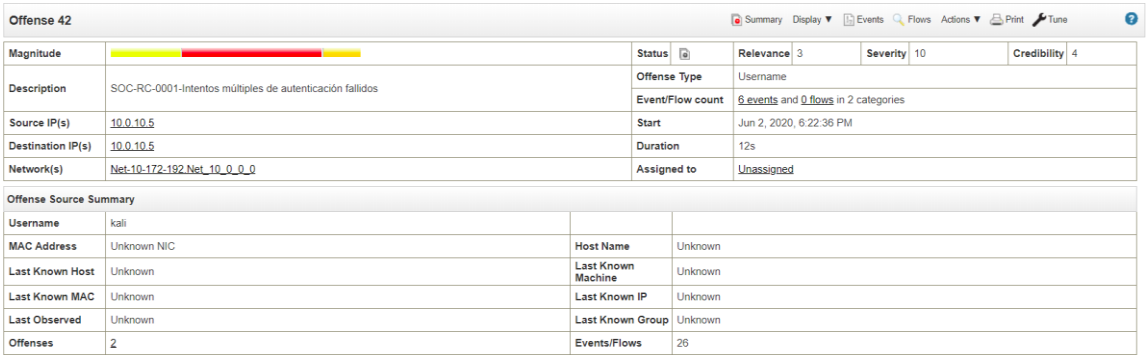
Análisis de la ofensa:

El analista SOC 1 se asigna la alerta a sí mismo, y comienza a verificar la información con ayuda del libro de reglas asignado a esa regla.

- La fuente de logs coincide con la IP de origen y destino, por lo que los intentos se han realizado directamente desde el dispositivo.
- El número de intentos fallidos se verifico: 4 intentos en total, seguidos de un login correcto y acceso al dispositivo.
- Se identifica el usuario: el usuario es “kali”, el cual es a la vez administrador del dispositivo.
- El usuario relacionado con la alerta es un administrador de sistemas Linux, lo cual tiene sentido para esta cuenta.
- En este caso, al no haber sospecha de un ataque de fuerza bruta, se contacta con el usuario directamente para verificar la actividad mediante un correo electrónico.
- El usuario contesta unos minutos más tarde informando acerca de un error introduciendo la contraseña, por lo que es un fallo humano.

Información encontrada por el analista:

- Numero de ofensa: 42
- Tiempo de comienzo de la actividad: Jun 2, 2020, 6:22:36 PM
- Tiempo del comienzo del análisis: Jun 2, 2020, 8:30:00 PM
- Duración: 12s
- Asignado a: Analista SOC 1
- Dirección de origen: 10.0.10.5 (kali)
- Dirección de destino: 10.0.10.5 (kali)
- Log source: Kali Linux Red Team



Offense 42

Summary | Display | Events | Flows | Actions | Print | Tune

Magnitude		Status		Relevance	3	Severity	10	Credibility	4
Description	SOC-RC-0001-Intentos múltiples de autenticación fallidos	Offense Type	Username						
		Event/Flow count	6 events and 0 flows in 2 categories						
Source IP(s)	10.0.10.5	Start	Jun 2, 2020, 6:22:36 PM						
Destination IP(s)	10.0.10.5	Duration	12s						
Network(s)	Net-10-172-192.Net_10_0_0_0	Assigned to	Unassigned						

Offense Source Summary

Username	kali		
MAC Address	Unknown NIC	Host Name	Unknown
Last Known Host	Unknown	Last Known Machine	Unknown
Last Known MAC	Unknown	Last Known IP	Unknown
Last Observed	Unknown	Last Known Group	Unknown
Offenses	2	Events/Flows	26

Figura 48. Imagen del sumario de la alerta 42

- Conclusión:

  El usuario ha realizado en uno de los dispositivos bajo su control un error en la autenticación debido a un fallo humano, no es necesario proceder más allá, la alerta puede ser cerrada.

- Acción siguiente:

  En este caso la ofensa puede ser cerrada, ya que la actividad no es un posible incidente de seguridad. Cerrando la alerta como “no sospechoso”

2.15.2 SOC-RC-0002-Comandos sospechosos ejecutados

Contexto en la empresa:

Los SIEM detectan que una cuenta en un sistema Windows está ejecutando comandos sospechosos de forma muy seguida en un dispositivo de usuario (Windows 10). El usuario encontrado no es muy técnico, por lo que inmediatamente elevan las sospechas sobre la actividad.

Se decide contactar con el usuario, el cual confirma que no estaba trabajando en el momento de la actividad. El analista decide escalar la ofensa al equipo de respuesta, para que procedan a bloquear el dispositivo y la cuenta asociada.

Poco después el equipo de respuesta recibe información de que se estaba generando un ejercicio de pentesting; la cuenta detectada era parte de la forma de acceder

Análisis de la ofensa:
El analista SOC 1 comienza a verificar la información con ayuda del libro de reglas asignado a esa regla.

- Los comandos analizados y detectados son los siguientes:

    - Cmd.exe
    - Whoami.exe
    - Svchost.exe
    - Ipconfig.exe

- Se verifican los comandos antes y después. No se aprecia mucha más actividad, pero sí que se relacionan con la alerta muchos intentos de intrusión desde otra máquina Linux en la red.

- El usuario es el mismo que el que utiliza el dispositivo de manera frecuente, por lo que, si hay actividad sospechosa, puede ser que la cuenta de usuario haya sido comprometida.

- Lo comandos han sido llamados desde línea de comandos directamente, lo que reafirma la sospecha de cuenta comprometida.

- El usuario que utiliza esta cuenta pertenece al departamento financiero, por lo que no es un usuario técnico. De nuevo más sospechas acerca de la actividad.

- Se contacta con CIRT de forma paralela para informar y preparar el envío del caso. El equipo confirma que se contacte con el usuario para comprobar si estaba utilizando el equipo en este punto. El usuario confirma que no se encontraba trabajando cuando la actividad ocurrió.

- El analista completa la información obtenida y envía el caso a l equipo de respuesta, que seguirá desde este punto.

Información encontrada por el analista:

- Numero de ofensa: 41
- Tiempo de comienzo de la actividad: Jun 2, 2020, 5:50:3617 PM
- Tiempo del comienzo del análisis: Jun 2, 2020, 6:50:00 PM
- Duración: 1:36 horas
- Asignado a: Analista SOC 3
- Dirección de origen: 10.0.10.4 (MSEDGEWIN10)
- Dirección de destino: 10.0.10.4 (MSEDGEWIN10)
- Log source: WindowsAuthServer @ MSEDGEWIN10

- <u>Conclusión:</u>

    La actividad parece no relacionada con el usuario, este ha confirmado que no poseía acceso al sistema en ese momento, la cuenta parece estar comprometida.

- Acción siguiente:

Se asigna la alerta al equipo de respuesta: CIRT, enviando un mail con la información del caso para continuar con la investigación. Se contacta con el miembro de guardia del equipo para comenzar la investigación cuanto antes.

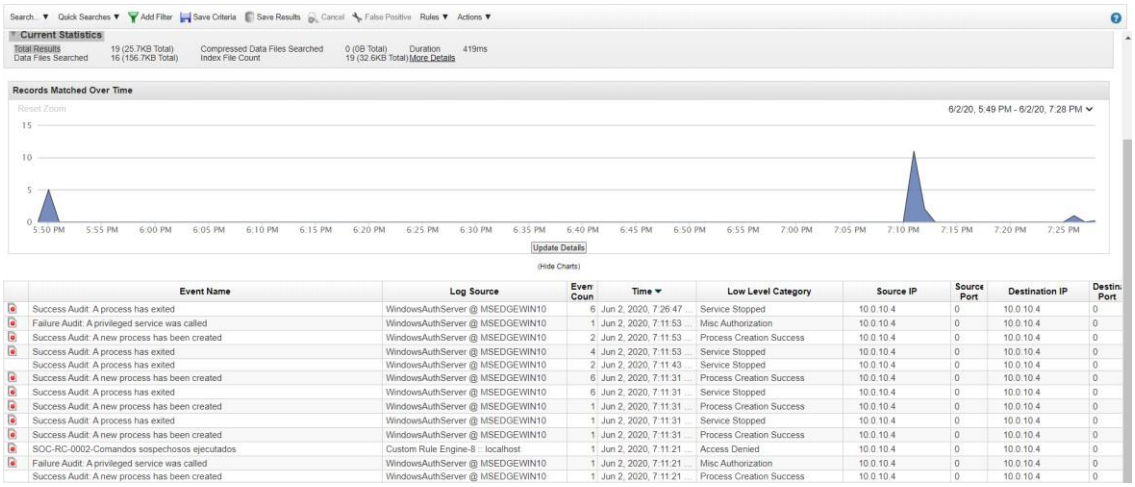


Figura 49. Eventos creados que muestran los comandos ejecutados.

2.15.3 SOC-RC-0003-Eventos no llegan desde endpoints

Contexto en la empresa:

Los eventos de un dispositivo en la red no llegan al SOC, al poder estar perdiendo información, se requiere que se informe al equipo de redes para verificar el problema.

Análisis de la ofensa:

En este caso la alerta solamente informa de que los eventos no están llegando, se debe verificar con el libro de reglas los pasos siguientes:

- Se comprueba, con una búsqueda, que el sistema sigue sin enviar eventos.

- Se comprueba que no hay ningún incidente de red en curso, para observar si no puede estar relacionado. Existe una ventana de mantenimiento de servidores en ese tiempo. Esta podría ser la causa.

Event Information

Event Name	SOC-RC-0003-Eventos no llegan desde endpoints						
Low Level Category	Warning						
Event Description	Se ha detectado que el dispositivo no envia eventos						
Magnitude	(8)	**Relevance**	6	**Severity**	10	**Credibility**	10
Username	N/A						
Start Time	Jun 3, 2020, 8:03:11 PM	**Storage Time**	Jun 3, 2020, 8:03:11 PM	**Log Source Time**	Jun 3, 2020, 8:03:11 PM		
CRE Description (custom)	Se ha detectado que el dispositivo no envia eventos Log source 'WindowsAuthServer @ MSEDGEWIN10' has stopped emitting events						
CRE Name (custom)	SOC-RC-0003-Eventos no llegan desde endpoints						
Domain	Default Domain						

Figura 50. Evento que informa que los logs no son recibidos.

- Se realiza una búsqueda de los últimos eventos enviados, para descartar que no haya actividad sospechosa, no la hay en este caso.

El analista envía un correo al equipo de red, el cual confirma que el sistema está en mantenimiento durante este tiempo, por lo que la actividad está aprobada.

Información encontrada por el analista:

- Numero de ofensa: 48
- Tiempo de comienzo de la actividad: Jun 3, 2020, 8:03:11 PM
- Duración: 4:18 horas
- Asignado a: Analista SOC 2
- Dirección de origen: 10.0.10.8 (localhost – el sistema alertador - Qradar)
- Dirección de destino: 10.0.10.8 (localhost – el sistema alertador - Qradar)
- Log source: localhost

Conclusión:
Información de la alerta enviada al equipo NOC. Confirman que han recibido otro email directamente de Qradar alertándoles de lo mismo. Confirman que la actividad es parte de un mantenimiento en la red.

Acción siguiente:

La alerta puede cerrarse como “No maliciosa”

2.15.4 SOC-RC-0004-Posible escáner de red detectado (Local-Local)

Contexto en la empresa:

Se detecta un posible escáner entre dispositivos locales. Este tipo de alertas pueden indicar que la máquina de origen está infectada o alguna actividad de reconocimiento se está llevando a cabo. Después de verificar los elementos de la alerta, parece que en este caso el dispositivo es legítimo, perteneciente al equipo de vulnerabilidad, pero la alerta no ha sido actualizada. El analista crea una petición para añadir la IP de origen a la lista de exclusiones de la regla de acuerdo con el procedimiento de modificación de reglas creado.

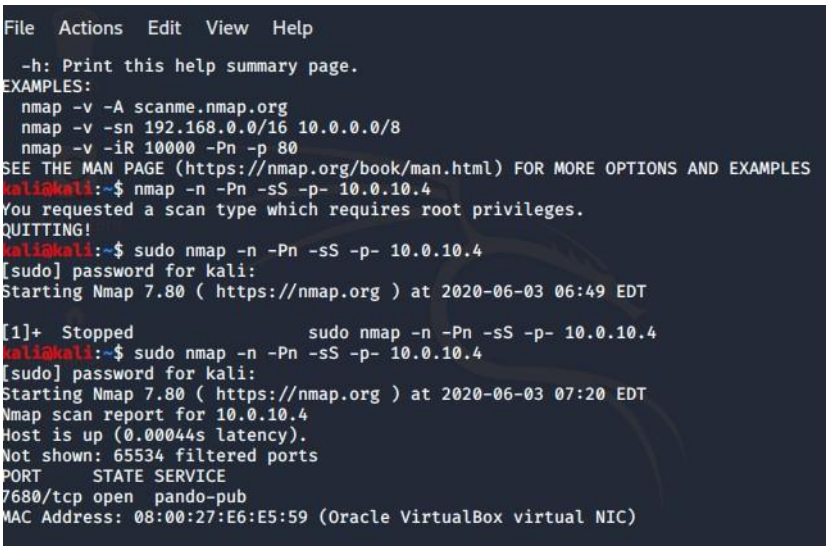


Figura 51. Imagen del escáner Nmap ejecutado para la alerta.

Análisis de la ofensa:

El analista requiere de los pasos descritos en el libro de reglas para comprobar al 100% que no hay ningún dato obviado que pueda hacer perder información. Los pasos analizados son los siguientes:

- Se comprueba que el dispositivo de origen corre sobre un sistema Linux.
- El dispositivo de destino es un servidor Windows.
- La actividad fue detectada durante una media hora, terminada cuando el analista comenzó su verificación.
- Se realiza una búsqueda de los últimos eventos enviados, para descartar que no haya actividad sospechosa, no la hay en este caso.
- Se verifican los eventos de la misma IP de destino, parece que se la IP no tiene mucha actividad previa en la red.
- El analista comprueba la lista de dispositivos de la red que realizan escaneos internos frecuentes, pero la IP indicada no se encuentra en la lista.
- Uno de los eventos muestra que uno de los puertos ha dado respuesta, por lo que la IP sabe que uno de los puertos está abierto.

Como última acción el analista contacta con el equipo de vulnerabilidades, y recibe confirmación de que se trata de un nuevo escáner de red implantado muy recientemente, por lo que no ha sido añadido a la exclusión. El caso a partir de que puede ser cerrado, pero una petición de modificación de regla debe hacerse para que esta IP no vuelva a generar alertas en el futuro.

Información encontrada por el analista:

- Numero de ofensa: 46
- Tiempo de comienzo de la actividad: Jun 3, 2020, 2:56:39 PM

- Duración: 34 minutos.
- Asignado a: Analista SOC 1
- Dirección de origen: 10.0.10.5 (kali)
- Dirección de destino: 10.0.10.4 (MSEDGEWIN10)
- Log source: WindowsAuthServer @ MSEDGEWIN10

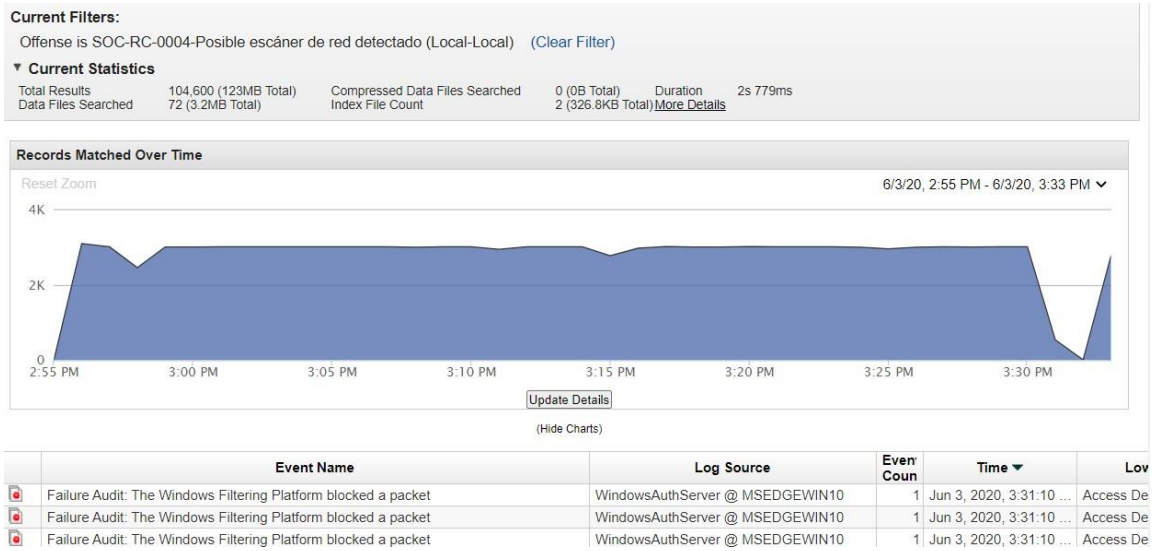


Figura 52. visión de la duración de los 100000 eventos en el gráfico.

Conclusión:

El escáner es legítimo y parte de la organización, en este caso la alerta es un falso positivo.

Acción siguiente:

La alerta puede cerrarse como “Falso positivo”. Seguidamente se creará una petición de cambio de la regla para incluir el nuevo escáner.

2.15.5 SOC-RC-0005-Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)

Contexto en la empresa:

Una regla monitoriza cuando se accede a una página no autorizada o que se encuentra en lista negra. La alerta se genera cuando uno de los usuarios accede a una página web externa, la página es la de la UOC. El usuario es contactado al no ver que la pagina sea peligrosa. El usuario confirma que el acceso se hizo fuera de horas de trabajo para verificar la documentación de una practica

Análisis de la ofensa:

El analista requiere de los pasos descritos en el libro de reglas para comprobar al 100% que no hay ningún dato obviado que pueda hacer perder información. Los pasos analizados son los siguientes:

- El dispositivo es un endpoint, por lo que ha sido un usuario sin administrador el que ha accedido.

- La reputación obtenida en los motores de análisis (virus total) no da ninguna alerta especifica. El analista utiliza un sandbox para verificar la web y parece relacionada con una universidad.

- El usuario es un técnico que trabaja en el departamento de seguridad.

- No se ven información transferida desde el ordenador de la empresa, pero si una descarga de datos.

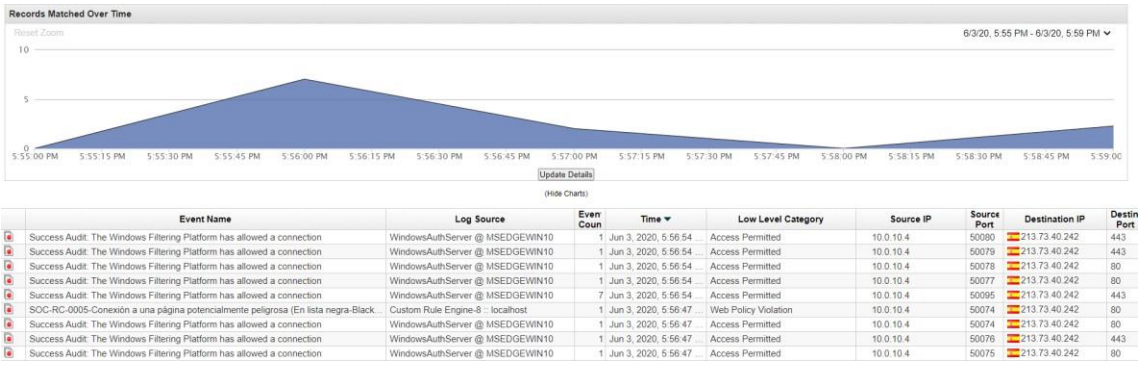
- No hay otras actividades sospechosas, pero si hay navegaciones a páginas no relacionadas con el trabajo, como periódicos deportivos.

- No existe historial de conexión a la página anteriormente.

Como no se observa actividad sospechosa, se decide contactar con el usuario. Este confirma que necesitaba verificar una información de la Universidad, por lo que al finalizar la jornada descargo un archivo para verificar que estaba correcto. Se confirmó que la actividad no contiene información de la empresa. La alerta se cierra en este caso como violación de política de empresa.

- Numero de ofensa: 49
- Tiempo de comienzo de la actividad: Jun 3, 2020, 5:56:47 PM
- Duración: 1:07 horas
- Asignado a: Analista SOC 4
- Dirección de origen: 10.0.10.4 (MSEDGEWIN10)
- Dirección de destino: 213.73.40.242 (UOC Data Network)
- Log source: WindowsAuthServer @ MSEDGEWIN10

Conclusión:
La actividad está confirmada como no maliciosa. Se ha informado al usuario que no realice este tipo de conexiones desde la red del trabajo, para evitar este tipo de alertas. La IP ha sido añadida a la exclusión de la regla.
Acción siguiente:
La alerta puede cerrarse como “violación de política de empresa”. Seguidamente se creará una petición de cambio de la regla para incluir la IP, ya que no es sospechosa.



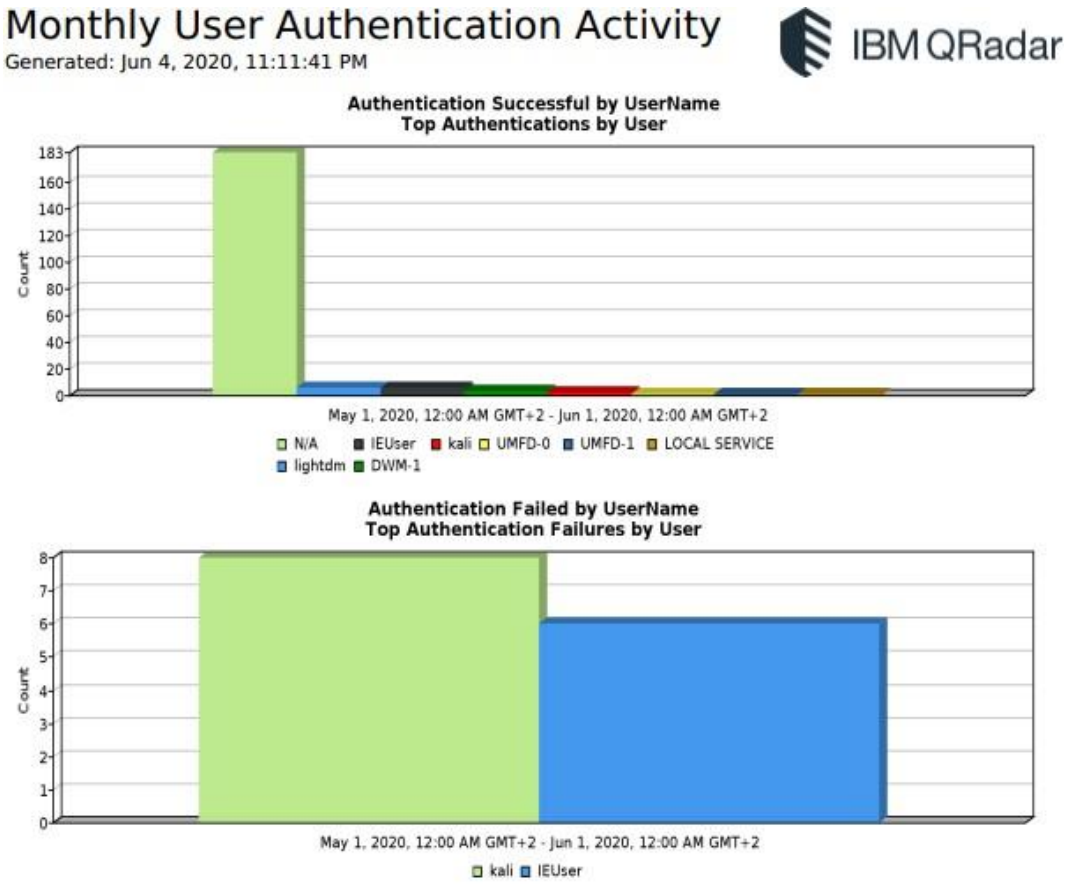
	Event Name	Log Source	Even Coun	Time	Low Level Category	Source IP	Source Port	Destination IP	Destin Port
	Success Audit: The Windows Filtering Platform has allowed a connection	WindowsAuthServer @ MSEDGEWIN10	1	Jun 3, 2020, 5:56:54 ...	Access Permitted	10.0.10.4	50080	213.73.40.242	443
	Success Audit: The Windows Filtering Platform has allowed a connection	WindowsAuthServer @ MSEDGEWIN10	1	Jun 3, 2020, 5:56:54 ...	Access Permitted	10.0.10.4	50079	213.73.40.242	443
	Success Audit: The Windows Filtering Platform has allowed a connection	WindowsAuthServer @ MSEDGEWIN10	1	Jun 3, 2020, 5:56:54 ...	Access Permitted	10.0.10.4	50078	213.73.40.242	80
	Success Audit: The Windows Filtering Platform has allowed a connection	WindowsAuthServer @ MSEDGEWIN10	1	Jun 3, 2020, 5:56:54 ...	Access Permitted	10.0.10.4	50077	213.73.40.242	80
	Success Audit: The Windows Filtering Platform has allowed a connection	WindowsAuthServer @ MSEDGEWIN10	7	Jun 3, 2020, 5:56:54 ...	Access Permitted	10.0.10.4	50095	213.73.40.242	443
	SOC-RC-0005-Conexión a una página potencialmente peligrosa (En lista negra-Black...	Custom Rule Engine-8 :: localhost	1	Jun 3, 2020, 5:56:47 ...	Web Policy Violation	10.0.10.4	50074	213.73.40.242	80
	Success Audit: The Windows Filtering Platform has allowed a connection	WindowsAuthServer @ MSEDGEWIN10	1	Jun 3, 2020, 5:56:47 ...	Access Permitted	10.0.10.4	50074	213.73.40.242	80
	Success Audit: The Windows Filtering Platform has allowed a connection	WindowsAuthServer @ MSEDGEWIN10	1	Jun 3, 2020, 5:56:47 ...	Access Permitted	10.0.10.4	50076	213.73.40.242	443
	Success Audit: The Windows Filtering Platform has allowed a connection	WindowsAuthServer @ MSEDGEWIN10	1	Jun 3, 2020, 5:56:47 ...	Access Permitted	10.0.10.4	50075	213.73.40.242	80

Figura 53. Eventos de la conexión a la página de la UOC.

2.16 Estadísticas e informes para directiva y auditoria.

A la hora de informar a los auditores del estado del proyecto para su verificación, aparte de proveer de la documentación necesaria parte de los objetivos, se debe proponer un sistema de informes para verificar el número de alertas generadas, por ejemplo, o datos específicos de actividades en la red. Para ello se ha optado por esperar a tipo de información requerida, para generar un reporte en Qradar mostrando el tipo de dato requerido.

En este caso, se muestra en la figura 46 un ejemplo de toda la actividad para un mes de las autenticaciones divididas por usuario, además de una muestra de los que se han autenticado en más ocasiones.



Top Failures Details
Top Authentication Failures by User
May 1, 2020, 12:00:00 AM - Jun 1, 2020, 12:00:00 AM

Username	Log Source (Unique Count)	Event Name (Unique Count)	Low Level Category (Unique Count)	Source IP (Unique Count)	Destination IP (Unique Count)	Geographic Country/Region (Unique Count)	Event Count (Sum)	Count
kali	Multiple (2)	Multiple (2)	Multiple (2)	10.0.10.5	10.0.10.5	Other	18	8
IEUser	Multiple (2)	Multiple (2)	Multiple (2)	10.0.10.4	10.0.10.4	Other	12	6

Figura 54. Muestra de un informe generado en Qradar.

Este tipo de informes se puede generar basándose en cualquier regla, evento, campo o bloque de datos que el sistema posea, además de poder generar el informe de forma manual, o enviarlo por correo en el momento que se configure.

2.17 Valoración económica del trabajo

Una vez que se ha llegado a la fase final del proyecto, es momento de la verificación antes del cierre de los objetivos económicos del proyecto. No podemos afirmar que se ha conseguido todo si el presupuesto inicial ha terminado duplicándose. En el caso de este proyecto se contaba con una ventaja respecto a otro tipo de proyectos, y es que la mayoría de los gastos son fijos o predispuestos por la empresa.

Un ejemplo claro de esto son los gastos de personal. Si tenemos en cuenta que, exceptuando un gasto de un consultor requerido para soporte de ingeniería, el resto del departamento está compuesto por empleados a tiempo completo, por lo que el gasto ya estaba contemplado de antemano (exceptuando horas extras).

Otro gasto relativamente contenido es el que se refiere a los productos implantados. En el caso de Qradar se cuenta con licencias predefinidas que se cargan a los presupuestos de forma anual, incluyendo casos de desviaciones de presupuesto, pero en este caso hacia abajo (debido al volumen contratado se rebaja el precio total). Para Splunk incluso se ha adquirido una licencia permanente, pudiendo ampliarla en el futuro con más tráfico, pero eso queda fuera del presupuesto de este proyecto inicial.

Por todo ello, podemos ver en la siguiente figura el desglose obtenido para el presupuesto del proyecto. Se ha optado por incluir solamente la parte de la implementación de la empresa, la parte que concierne a la red de pruebas a generado un gasto que no llega a los 10 euros, por lo que se ha dejado fuera.

Presupuesto proyecto FinComp

Coste fijos

Concepto	unidades	Precio unidad (euros)	Requerido por	Inicio	Final	total (dias de trabajo)	Coste estimado (Euros)	Coste real (Euros)	Desviación (Euros)
Implementación Qradar	1		FinComp	09-03-20	01-06-20	108	520000	520000	0
Compra hardware - Consola	1	0	FinComp	09-03-20	01-06-20	0	0(con licencia)	0	0
Compra hardware - Colectores	11	20000	FinComp	09-03-20	25-06-20	108	110000	110000	0
Compra hardware - Procesadores adicionales	4	40000	FinComp	09-03-20	25-06-20	108	160000	160000	0
Compra software - Licencia (25000 EPS)	1	250000	FinComp	09-03-20	09-03-21	365	250000	250000	0
Implementación Splunk	1		FinComp	09-03-20	01-06-20	108	310000	310000	0
Compra hardware - Consola	1	0	FinComp	09-03-20	01-06-20	0	0(con licencia)	0	0
Compra hardware - Colectores	3	20000	FinComp	09-03-20	25-06-20	108	60000	60000	0
Compra software - Licencia (100 GB/día)	100	2500	FinComp	09-03-20	permanente	N/A	250000	250000	0
Coste mano de obra	10		FinComp	01-03-20	01-07-20	180	354000	354000	0
Ingenieros SOC	2	80000	FinComp	01-03-20	01-07-20	180	80000	80000	0
Analistas SOC senior	2	75000	FinComp	01-03-20	01-07-20	180	75000	75000	0
Analistas SOC junior	4	65000	FinComp	01-03-20	01-07-20	120	104000	104000	0
Service Delivery Manager	1	90000	FinComp	01-03-20	01-07-20	180	45000	45000	0
SOC Manager	1	100000	FinComp	01-03-20	01-07-20	180	50000	50000	0

Costes variables

Concepto	unidades	Precio unidad (euros)	Requerido por	Inicio	Final	tiempo total (dias de trabajo)	Coste estimado (Euros)	Coste real (Euros)	Desviación (Euros)
Empleo ingeniero extra (consultor)	20 días	500	SOC	20-04-20	22-05-20	20	0	10000	10000
Horas extra ingeniería - producción	100 horas	100	SOC	02-05-20	02-05-20	1.2	0	10000	10000
Soporte del departamento de redes para ayuda con la infraestructura	150 horas	100	SOC	09-03-20	01-06-20	6.25	0	15000	15000

Total estimado	1184000
Total real	1219000
Desviación total	35000

Figura 55. Presupuesto para el proyecto presentado.

Como vemos, la mayor parte del presupuesto, casi la mitad de éste, se lo lleva la adquisición de materiales para la implementación de Qradar. El coste de implementación se dispara en el momento que se necesitan añadir colectores y procesadores extra.

La licencia tampoco se queda atrás en este sentido, y aunque sí que incluye el soporte de IBM para implementaciones y problemas con el hardware/software, su elevado precio hace que solo grandes compañías puedan permitirse este tipo de infraestructuras. En esta primera adquisición se ha optado por seleccionar un límite de 25000 eventos por segundo, los cuales seguramente sean demasiados, pudiendo renegociar el próximo año un número menor de estos por un precio más bajo.

En lo que corresponde a Splunk, el precio se rebaja bastante, esto es debido a que se requiere de menos infraestructura, ya que va a ser implementado más como apoyo que como herramienta principal.

Esto precios estaban pactados de antemano, por lo que no se ha producido ninguna desviación de lo establecido en este caso.

Para la mano de obra empleada, se han establecido valores de coste brutos. Obviamente el mayor gasto se lo lleva el director, y en conjunto, los 6 analistas del proyecto. Su sueldo es elevado al tener que trabajar las 24 horas, por lo que se han incluido gastos por nocturnidad y fines de semana.

Con los costes fijos del proyecto se ha alcanzado un total de 1.184.000 euros, a estos costes le tendremos que añadir los siguiente, los cuales no eran esperados:

1. 30 días naturales (20 días de trabajo) de un consultor externo para soporte de los trabajos de ingeniería. Este tipo de consultores se pagan por día trabajado.

2. Horas extra de ingeniería para realizar instalaciones en horarios fuera de oficina. Aquí entran las horas necesarias para introducir los SIEM en producción.

3. Horas extra del departamento de redes para la implementación del envío correcto de todos los dispositivos a los SIEM. Se han calculado 150 horas divididas por todos los miembros del equipo durante todo el proyecto.

El total conjunto de estos gastos variables asciende a 35.000 euros. Esto significa que no se hemos desviado del presupuesto inicial un 2.95%, lo cual es un muy buen margen de desviación. En este caso el presupuesto debería aprobarse sin mayores complicaciones por parte del cliente.

2.18 Cierre del proyecto

2.18.1 Entregables proporcionados

Vamos a observar primeramente los entregables que se nos habían pedido para el final del proyecto, para comprobar cuales han sido entregados, cuales están pendientes y cuales se han cancelado:

Entregables (Operaciones)

- Diagrama de Gantt (Completado): Se entrega con todas las dependencias, tareas y objetivos definidos.

- Entrega de los casos de uso creados o plantillas relacionadas (Completado): El procedimiento de creación de casos de uso además de 5 casos de ejemplo han sido entregados.

- Entrega de la documentación de las reglas creadas (Completado).

- Entrega de los Playbooks creados y verificados (Completado).

- Entrega de reportes con las estadísticas de las operaciones (Cancelado - alternativa): Se ha optado por mostrar la herramienta de reportes que los SIEM poseen, para que, en caso de una petición por parte de os auditores, se pueda extraer información directamente del SIEM.

Entregables (Gestión)

- Disaster recovery plan para el SOC (Completado)
- Monitorización de alertas (Completado): Cómo realizar una monitorización correcta de las alertas generadas en los SIEM
- Escalación (Completado): Como proceder en caso de que una alerta generada sea clasificada como un potencial incidente de seguridad.
- Modificación de reglas (Completado): Pasos para modificar correctamente una regla existente en los SIEM
- Plan de entrenamiento para miembros del SOC (Completado)
- Toda la documentación referente a las reuniones que se produzcan durante el proyecto, por razones de verificación y responsabilidad en las decisiones tomadas (Completado).

Como se puede ver, se ha cumplido prácticamente con todos lo entregables requeridos, el único caso en el que se ha realizado una modificación ha sido en los informes y estadísticas, ya que se ha considerado que no se puede crear un procedimiento estándar, dado el amplio espectro de tipos de peticiones que pueden llegar. Podemos afirmar que la sección de entregables ha sido completada exitosamente en tiempo y forma.

2.18.2 Objetivos del proyecto

En lo que respecta a los objetivos planteados al inicio, podemos decir que en general se han cumplido correctamente:

Se ha logrado implantar mediante la organización del proyecto las herramientas hardware en cada una de las zonas propuestas, incluyendo (aunque al final del proyecto) los elementos en la zona de Producción. Por supuesto que es una instalación inicial, ya que las posibles mejoras o aumento de sistemas deben ser cubiertos a posteriori.

El sistema se ha implementado pensando en la disponibilidad. Tal como se ha diseñado la red de colectores y procesadores, no existe un riesgo elevado de perder la comunicación de forma accidental, ya que muchas de las configuraciones son de alta disponibilidad. Se ha incluido, como mencionamos en los entregables, un procedimiento de respuesta ante desastres, que ayudará a actuar rápido y a minimizar el daño en caso de que el sistema no está disponible.
Se ha llevado a cabo un test final (el correspondiente con la sección 2.15 de la memoria) donde se prueba a los auditores que el SOC está preparado para una respuesta en tiempo y forma a las alertas generadas en el sistema, por lo que a partir del cierre del proyecto, Fincomp podría operar de forma autónoma, sin dependencia del equipo de

proyecto. Cabe destacar que muchos de los componentes del equipo han recibido la oferta de continuar por lo que el departamento permanecería como está por el momento, sin grandes cambios en la plantilla.

3. Conclusiones

Para finalizar el presente proyecto, se van a mostrar las conclusiones generales, lecciones aprendidas, aspectos a mejorar y una valoración general del proyecto realizado.

En general, podemos afirmar con todos los datos obtenidos que ha cumplido con los objetivos. Si bien es verdad que una parte del proyecto no ha podido ser completada al 100% como se esperaba al principio del proyecto (informes y estadísticas), el resto se ha podido completar de manera satisfactoria.

Si que cabe mencionar también un aspecto negativo a mejorar, ya que no se ha dedicado tanta atención a Splunk como se la ha dado a Qradar, esto viene por dos razones principales:

A. El conocimiento del producto era mucho más limitado que el de Qradar, y una vez comenzado el proyecto se ha visto que no iba a ser posible crear una versión dual con ambas herramientas repartiéndose un 50% del proyecto. Se ha optado por sacrificar parte de la implementación de Splunk en las explicaciones en favor de Qradar, para agilizar el resto de las secciones del proyecto.

B. La versión gratuita de Splunk (Splunk Phantom) no admite directamente la inserción y creación de reglas, para ello otra versión de Splunk debía ser añadida. Este punto elevaría la dificultad de la implementación de la red bastante, por los que se optó por le envío de las alertas directamente desde Qradar a Phantom.

Con todas las tareas finalizadas, es buen momento para reunir las lecciones aprendidas del proyecto, de modo que, si en un futuro una tarea así se repite, se podrán observar y tratar de mejorar los aspectos mencionados:

Quizás en el proyecto de la empresa se debería haber dejado un tiempo inicial mayor para la implementación del hardware y las configuraciones. Se decidió posponer casi un mes el comienzo de la implementación de hardware, lo cual lastró el avance del resto del proyecto, teniendo que dedicar recursos extras para el soporte de la carga de trabajo de ingeniería, cayendo en gastos extras inesperados.

En lo que concierne a la creación de la red de pruebas, debido a la no preparación y la verificación del material necesario se incurrió en la instalación y configuración de elementos que al final fueron descartados, haciendo perder tiempo de implementación para el resto del proyecto.

Por último, a nivel personal, el proyecto ha supuesto una mejora en los conocimientos de la administración y procesos de un SOC. Tanto con la información adquirida con la bibliografía como con los consejos de mis compañeros del SOC he visto un enfoque de mi trabajo más relacionado con la gestión, lo cual da una perspectiva de todo el trabajo que hay alrededor de uno de estos departamentos.

4. Glosario

- **Activo-activo:** Este término se utiliza sobre todo en implementaciones de alta disponibilidad, en la que dos máquinas funcionan una activa y la otra en estado de espera, verificando cuando la máquina primaria se desactive para obtener el rol principal.

- **Activo-pasivo:** Este término se utiliza para configuraciones de alta disponibilidad. En este tipo de configuración todos los dispositivos se encuentran activos, repartiéndose las tareas normalmente al 50%, aunque esto puede ser configurable.

- **Building block:** Bloque de información que contiene una serie de condiciones para que una regla se active. Como puede ser una serie de instrucciones o comandos.

- **CIO:** *Chief Information Officer*. Responsable de las tecnologías de la información de una empresa. Responde ante el consejo de administración y el presidente.

- **CISO:** *Chief Information Security Officer.* Responsable de la sección especifica de la seguridad aplicada a las tecnologías de la información. Responde ante el CIO.

- **DDoS:** *Distributed Denial of Service* o ataque de denegación de servicio distribuido. En un tipo de ataque donde se envían múltiples peticiones de acceso a un servicio con el objetivo de colapsar la entrada y denegar el acceso a usuarios legítimos del sistema.

- **DHCP:** *Dinamyc Host Control Protocol*. Protocolo de red que permite que un dispositivo que se conecta a la red obtenga una dirección de red dentro de un rango especificado, sin necesidad de tener que configurar una IP de forma manual.

- **DMZ:** *Demilitarized zone*. Zona de la red que se sitúa normalmente como frontera entre las IPs externas que se comunican con Internet y las IPs internas de una compañía. Suelen albergar los gateways de acceso a las plataformas de cliente.

- **DNS:** *Domain Name System.* Es un sistema de nombres que actúa de forma jerárquica y asigna nombres de dominio a direcciones de red.

- **Equipo azul (Blue Team):** En ciberseguridad, este término se emplea para denominar al equipo del SOC (defensivo y respuesta). Este equipo se encarga de la monitorización y defensa, creando acciones de búsqueda de actividad sospechosa en la red.

- **Equipo púrpura (Purple Team):** Este equipo nace de la fusión de los equipos azul y rojo. Se denomina a un equipo púrpura cuando existe colaboración entre las dos partes de un test de vulnerabilidades, colaborando para reforzar la seguridad de la red.

- **Equipo rojo (Red Team):** Este equipo de personas es el encargado de detectar agujeros en la configuración de seguridad de una red, intentando explotarlos para ganar acceso a recursos de la red. Estos equipos se los denomina también pentesters. Normalmente no existe mala intención detrás de sus acciones. Éstas se realizan de forma preventiva para evitar que un ataque real suceda.

- **Falso negativo:** En detección de alertas, se refiere a una alerta que debería haber sido generada o analizada, pero ha sido descartada como no peligrosa, cuando en realidad debería haber sido generada.

- **Falso positivo:** En detección de alertas, este término se refiere a una alerta que ha sido generada por el sistema, pero no debería haber aparecido, ya que no cumple las condiciones de la alerta. Suele deberse a fallos en la implementación de los parámetros de detección.

- **Flows:** En ciberseguridad hace referencia a un flujo de datos, normalmente relacionado con una actividad, mostrando la información directamente en lugar de ser procesada como un evento. Se podría considerar como un ¨pedazo¨ de la información transmitida.

- **FMI:** *Financial Market Infrastructure.* Este término hace referencia a compañías que, por su posición en el mercado, actúan como bases del sistema financiero, sistémicas y de las que dependen los mercados para operar.

- **Gantt diagram:** Diagrama que se diseña para mostrar la línea de tiempo de cada tarea que se ejecuta en un proyecto determinado.

- **Gateway:** El dispositivo que actúa como un Gateway en redes es el dispositivo que permite la comunicación entre dos redes distintas, actúa como puerta de entrada y-o salida en una comunicación de red.

- **GDPR:** *General Data Protection Regulation*, es el equivalente europeo de la Ley Orgánica de Protección de Datos (LOPD) que se aplica en España actualmente.

- **Hacking ético:** Técnicas de explotación de vulnerabilidades que tiene como fin reforzar la seguridad de la red de cara a un ataque real.

- **Heartbeat:** Señal utilizada normalmente por equipos conectados en alta disponibilidad. Esta señal se envía cada pocos segundos entre los dispositivos para verificar que siguen activos. Si esta señal se interrumpe un determinado número de veces, indicaría al dispositivo secundario que debe tomar el control.

- **High availability:** Forma de conexión lógica entre dispositivos similares que permite que dos o más de ellos se vean en la red como una sola unidad. Esto permite que, si uno de ellos falla, los consecuentes se activan, manteniendo las comunicaciones estables en la red.

- **IOC:** *Indicator of Compromise*. Valores que se asocian con actividad peligrosa para la red, o como indicador de elementos usados en ataques por actores maliciosos. Un IOC puede ser una IP, un comando, un programa, un virus…

- **ISO-27001:**https://ec.europa.eu/info/law/law-topic/data protection/reform/rules-business-and-organisations_en

- **KPI:** *Key Performance Indicator*. Indicador utilizado para valorar numéricamente un objetivo en un proyecto, se mide en valor absoluto.

- **Logs:** Evento creado por un dispositivo con la información del cambio que ha realizado en el sistema, se anota el tiempo, los dispositivos de origen y destino y otras informaciones.

- **NOC:** *Networking Operations Center*. Es el equivalente a un SOC, pero simplemente se centra en monitorizar la disponibilidad y seguridad de los elementos de red.

- **NTP:** *Network Time Protocol.* Protocolo de red que permite sincronizar los sistemas con relojes atómicos alrededor del mundo. Insertando la dirección del reloj que se desea, el dispositivo toma la misma hora como la hora del sistema.

- **Out of the box:** Término que hace referencia al funcionamiento de un sistema al ser configurado por defecto, o como su nombre indica, al sacarlo de la caja.

- **Out-of-scope:** Término que hace referencia a una acción que no se encuentra dentro de las tareas de un equipo o dispositivo, por lo tanto, no puede o debe ser realizada.

- **Parsing:** Concepto que hace referencia a la ordenación de los elementos de un paquete en elementos que hacen más fácil su comprensión.

- **Pentesting**: Ver términos Hacking ético o equipo rojo.

- **Playbook:** Conjunto de instrucciones a seguir paso a paso por un analista de un SOC para tratar una alerta especifica generada en los sistemas de monitorización.

- **Port Forwarding:** Este concepto es una aplicación de la traducción de puertos o NAT, con este sistema se traduce un puerto a otro de forma interna, para poder acceder a un servicio que utiliza un puerto conocido a través de un puerto privado.

- **Reference Set:** Lista que contiene una serie de parámetros a analizar para la detección de una regla, estos parámetros puede ser nombres, dominios, IPs, usuarios…

- **SDM:** Service Delivery Manager. Posición dentro del SOC con la tarea de contactar con los clientes o stakeholders del SOC para gestionar los posibles requerimientos para monitorizar casos de uso.

- **Shadowing:** Técnica en la que un nuevo miembro de un equipo se dedica a observar a otro miembro para aprender, sin realizar el trabajo, pero observando cómo hacerlo.

- **SLA:** *Service-level agreement*. Acuerdo entre partes para llevar a cabo un trabajo o proyecto en un tiempo determinado.

- **SOC*:*** *Security Operations Center*. Centro de monitorización de ciberamenazas.

- **SSH:** *Secure Shell.* Método de acceso remoto a consola donde, a diferencia de protocolo Telnet, los datos viajan cifrados.

- **Syslog:** Formato de envío de logs por defecto utilizado en sistemas con base Linux.

- **Tier:** Nivel de experiencia y responsabilidad en un puesto de trabajo, usualmente comienza en el nivel 1 (junior), aumentando el número dependiendo del puesto.

- **UBA:** User Behavior Analysis. https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.3.2/com.ibm.UBAapp.doc/c_Qapps_UBA_intro.html

- **Use Case (Caso de uso):** Posible escenario propuesto/requerido en el que se describe una posible amenaza a observar. En los casos de uso o use cases se debe contemplar cómo actuar si la amenaza mencionada aparece.

- **Wincollect:** Formato de envío de logs utilizado en sistemas Windows.

5. Bibliografía

- **Nota:** No toda la información empleada en la redacción de esta propuesta ha sido obtenida mediante referencias o bibliografía externa, sino que ha sido obtenida por la experiencia al trabajar en un proyecto similar

- Mokalled, Hassan, et al. “The Applicability of a SIEM Solution: Requirements and Evaluation.” 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2019 IEEE 28th International Conference on, WETICE, June 2019, pp. 132–137. EBSCOhost, doi:10.1109/WETICE.2019.00036.

- PR Newswire. “New Research From CRITICALSTART Finds That 8 Out Of 10 Security Analysts Report Annual Security Operations Center Turnover Is Reaching 10% To More Than 50%.” PR Newswire US, 29 Aug. 2019. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=bwh&AN=201908290830PR.NEWS.USPR. DA55230&site=eds-live&scope=site.

- Splunk Inc. “Splunk Mission Control Takes Off, Supercharging the Security Operations Center.” Business Wire (English), 2019 10AD. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=bwh&AN=bizwire.bw47806984&site=eds-live&scope=site.

- Al-Moshaigeh, Abdullah, et al. “Cybersecurity Risks and Controls.” CPA Journal, vol. 89, no. 6, June 2019, pp. 36–41. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=bth&AN=136901848&site=eds-live&scope=site.

- https://developer.ibm.com/qradar/ce/130034 **- instalación de Qradar (máquina virtual) (inglés).**

- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations_en - **Ley de protección de datos (GDPR) aplicada a empresas generada en la web de la comisión europea. (inglés).**

- https://hackernoon.com/complete-guide-on-soc-and-its-implementation-for-your-business-37b063cb9128 - **guía para la Implementación de un SOC para empresas. (inglés).**

- https://www.splunk.com/en_us/form/the-fundamental-guide-to-building-a-better-security-operation-center-soc.html **- guía de las mejores prácticas para implementar un SOC (inglés).**

- https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.3/com.ibm.qradar.doc/b_qradar_qsg.html **- guía de instalación y configuración de Qradar (inglés).**

- https://www.splunk.com/en_us/form/the-present-and-future-of-security-operations.html **- Mejores prácticas en ciberseguridad propuestas por Splunk (inglés)**

- https://www.ibm.com/security/artificial-intelligences **- Explicación de la IA Watson para SIEM implementada por IBM (inglés)**

- https://www.realcleardefense.com/articles/2019/11/25/assessing_north_koreas_cyber_evolution_114869.html **- Recopilación de información del grupo Lazarus desde su primera aparición (inglés)**

- https://blog.eccouncil.org/5-emerging-cyber-threats-to-watch-in-2020/ **- Las amenazas más importantes a tener en cuenta de cara al año 2020 (inglés)**

- https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=IBM%20Security&product=ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.3.0&platform=All&function=textSearch&text=wincollect **– Acceso a IBM BigFix para la obtención del instalador de Wincollect en Windows, (inglés).**

- https://exchange.xforce.ibmcloud.com/hub – **Descarga de los complementos para Qradar de la web de aplicaciones de IBM Xforce, (inglés)**

- https://www.lenovo.com/es/es/laptops/thinkpad/p-series/ThinkPad-P50/p/22TP2WPWP50 **– Información e imágenes del ordenador portátil utilizado para la realización del proyecto.**

- https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/c_qradar_deployment_guide_arch.html **– Desglose de las partes del hardware de Qradar (inglés).**

- https://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/t_qradar_create_cust_rul.html **– Guía para crear una regla personalizada en Qradar. (inglés).**

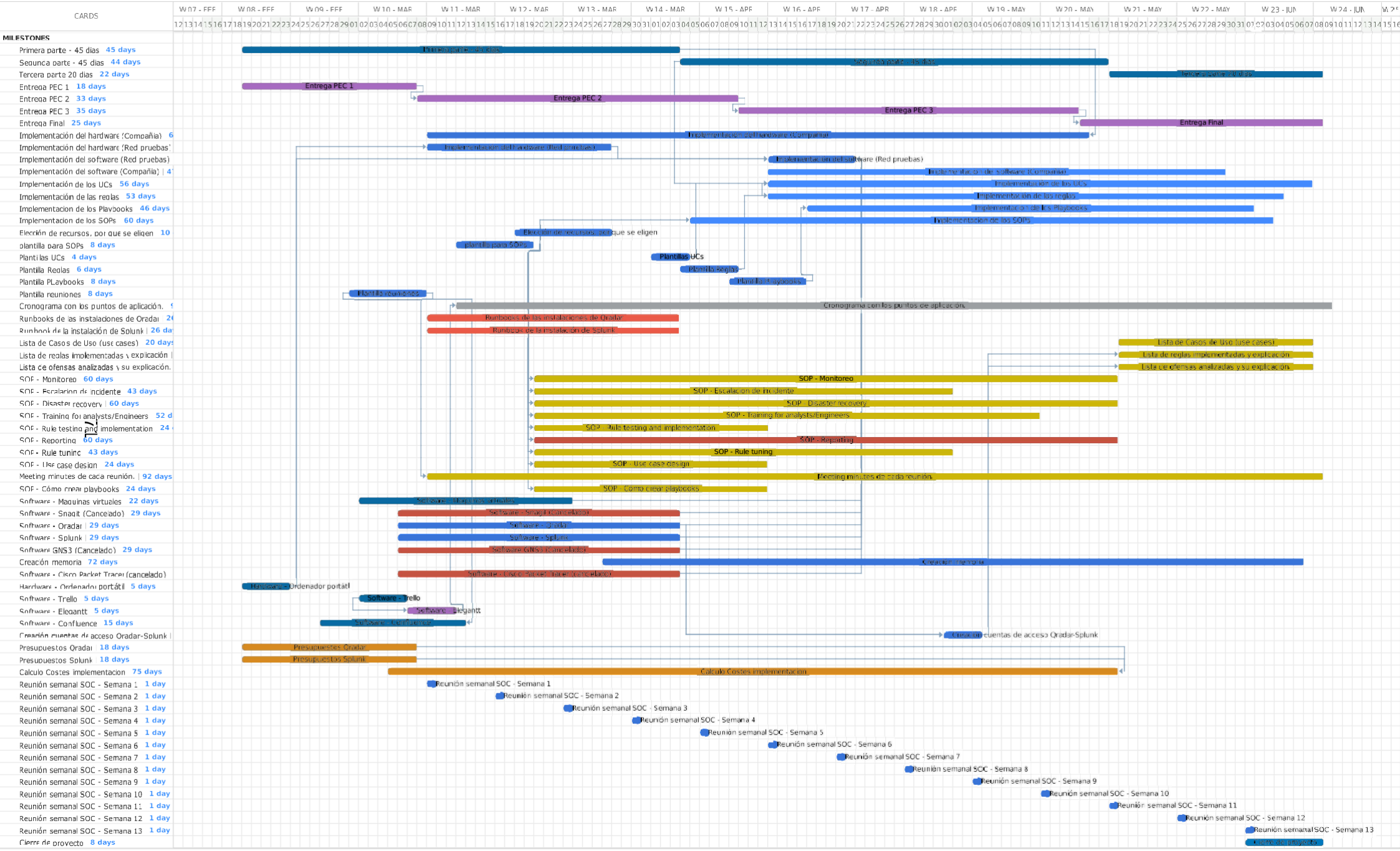
- https://www.learnsplunk.com/splunk-pricing---splunk-licensing-model.html **– Obtención de orientación para el cálculo del presupuesto de Splunk (datos modificados). (inglés).**

- http://www.reydes.com/d/?q=Escanear_Todos_los_Puertos_de_un_Host_utilizando_Nmap **– Verificaión para la utilización de Nmap en Kali Linux. (inglés).**

6. Anexos

Todos los anexos han sido desarrollados con la herramienta de Gestión Confluence. Se han exportado todos los archivos creados en PDF y se adjuntan a continuación. Existe un acceso al programa para verificar cada documento si fuera necesario.

TFG SOC coordinacion



SOC-SOP-0006-Monitorización de alertas

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	20 Mar 2020
Requerido por	SOC, auditores, Fincomp
Fecha límite de activación	18 May 2020
Creador	Analista SOC
Responsable	@ Daniel Rodríguez Fueyo
Última fecha de revisión	17 May 2020

Tabla de revisiones del documento

Versión actual del documento	1.0
Fecha de modificación	17 May 2020
Editor	@ Daniel Rodríguez Fueyo
Persona que ha aprobado los cambios	Analista SOC
Última fecha de aprobación	17 May 2020

Introducción al procedimiento

Una vez que las alertas se generan en los SIEM, el analista debe priorizar las alertas a tratar, y proceder a resolver el conflicto específico que se observa y proceder al cierre de la alerta o su escalación a un grupo superior si procede. Este procedimiento explicará de forma general los pasos a seguir en la monitorización de las alertas generadas por los SIEM.

Objetivo

Descripción de los pasos a seguir para realizar un análisis correcto de las alertas generadas en los SIEM.

> Para pasos más específicos, se deben consultar los libros de reglas asociados a cada una de las reglas.

Materiales requeridos

- Acceso de analista a Qradar.
- Acceso de analista a Splunk.
- Acceso a internet (para verificar información en fuentes externas (virus total, por ejemplo).

Desarrollo del procedimiento

Selección de las alertas

- **Dependiendo de la red:** Dependiendo de las alertas que se generen en un instante determinado, el analista deberá priorizar primeramente todas las alertas que afecten a equipos de la zona de producción, ya que, en caso de confirmarse como incidentes de seguridad, tendrían más impacto que en el resto de las zonas. La priorización debe seguir la siguiente lista:

1. Producción
2. Zona usuario
3. Zona DMZ
4. Zona SOC
5. Proxies y DNS
6. Zona SSL-VPN
7. Otras delegaciones
8. Zona test

- **Dependiendo del número de dispositivos afectados:** Se priorizan las alertas con más impacto en cuanto al número de dispositivos.
- **Dependiendo de si la actividad ha finalizado a sigue en proceso:** Si los eventos continúan agregando a la alerta, deben ser revisados.
- **Dependiendo de si se generan múltiples alertas similares o no:** En el caso de generarse alertas iguales se puede asumir que algo sospechoso está ocurriendo, y debe ser verificado.

Análisis de la alerta seleccionada

Una vez que el analista ha optado por una alerta (ofensa) específica, se deben seguir los punto especificados en el libro de reglas asignado a la regla que ha activado la alerta. En el libro de alertas se especifican los puntos críticos a analizar para cada una de las alertas, guiando al analista para la recopilación de información, escalación, o resolución del incidente según corresponda.

Toda la información será incluida como una nota en cada una de las alertas, ya que la información debe reflejarse para ser utilizada en caso de envío de la alerta a otro departamento o para su verificación por los auditores.

Referencias

SOC-SOP-0003-Entrenamiento para analistas

SOC-SOP-0007-Escalación de posibles incidentes de seguridad

SOC-SOP-0008-Modificación y mejora de reglas SIEM

SOC-SOP-0007-Escalación de posibles incidentes de seguridad

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	20 Mar 2020
Requerido por	SOC, Fimcomp, auditores
Fecha límite de activación	18 May 2020
Creador	Service Delivery Manager, Analistas senior
Responsable	@ Daniel Rodríguez Fueyo
Última fecha de revisión	01 May 2020

Tabla de revisiones del documento

Versión actual del documento	1.0
Fecha de modificación	30 Apr 2020
Editor	Analista senior 1
Persona que ha aprobado los cambios	@ Daniel Rodríguez Fueyo
Última fecha de aprobación	01 May 2020

Introducción al procedimiento

En caso de un posible incidente de seguridad, los analistas deben conocer cómo actuar y escalar el incidente a los departamentos o personas encargados de mitigarlos o eliminarlos. Para ello, se debe conocer el protocolo de actuación en caso de escalación, ya que podría variar dependiendo del tipo de alerta generada en los SIEM.

Objetivo

- Indicación de los pasos de escalación necesarios para departamentos específicos y dentro del SOC.

Activadores del procedimiento y afectados

Se enumeran a continuación los activadores y afectados por el procedimiento de escalación descrito:

Activadores	**Departamento /Puesto**	**Descripción**
Analistas del SOC	SOC (analistas)	Escalación mediante alertas del SIEM.
Afectados	**Departamento /Puesto**	**Descripción**
Analistas Tier 2 o Senior	SOC (analistas)	Escalación de alertas de los analistas Tier 1 en horario de oficina.
Ingenieros SOC	SOC (Ingeniería)	Escalación de alertas que afectan al rendimiento o configuración de los SIEM
Equipo de respuesta de seguridad	SOC-CIRT	Escalación de alerta s desde Tier 2 o Tier 1.
Responsables departamento	Otros departamentos de Fincomp	Escalación de alertas de los analistas Tier 2 o Tier 1.

Materiales requeridos

Acceso de analista a Qradar.

Acceso de analista a Splunk.

Desarrollo del procedimiento

Escalación genérica (sin impacto inmediato).

Una vez que los analistas han procedido a la selección y análisis de una alerta específica enviada al SOC, y se obtiene como resultado que la actividad puede ser un posible incidente de seguridad, **pero que no tiene un impacto inmediato o severo en la organización**, se debe enviar la información al departamento correspondiente o a las personas que puedan utilizar esta información para mitigar el suceso y eliminar el riesgo para la empresa. El procedimiento estándar para todos los casos genéricos sería el siguiente:

1. El caso se clasifica como posible incidente de seguridad
2. Se recoge toda la información relevante del caso, usando la información de los SIEM o con herramientas externas (verificación de reputación vía web, IOCs proporcionados por inteligencia…).
3. Escalar para obtener un análisis más detallado

- Si la actividad se produce en horario de oficina, se enviará a un analista senior de soporte (Tier 2).

La segunda línea de analistas, con más experiencia, serán los encargados de verificar, obtener información extra y mitigar las alertas en caso de que la actividad ocurra en el turno general. Se utiliza este sistema como filtro para no enviar un número elevado de alertas y colapsar los servicios de mitigación con posibles falsos positivos.

- Si la actividad se produce en un horario donde la oficina se encuentra cerrada, se enviaría la información a la persona senior del SOC de guardia, siempre con copia a la dirección.

Escalación con prioridad (impacto).

Si el caso detectado tiene impacto directo en la organización, pero no afecta a muchos de los sistemas o usuarios, se acelera el proceso de escalación, enviando directamente el caso al equipo CIRT, actuando los analistas de soporte en caso de que sean requeridos como soporte adicional en la investigación.

1. El caso se clasifica como posible incidente de seguridad medio
2. Se recoge toda la información relevante del caso, usando la información de los SIEM o con herramientas externas (verificación de reputación vía web, IOCs proporcionados por inteligencia…).
3. Escalación al equipo CIRT.
4. Actuación como soporte del equipo CIRT si se requiere, continuando con las labores diarias si no se comunica ningún cambio.

Escalación crítica (gran impacto).

En caso de que la organización se vea gravemente afectada, se realizaría una escalación inmediata al equipo CIRT, informando a la organización regularmente, y utilizando todos los recursos del SOC disponibles para centrarse en la alerta y cómo mitigarla.

1. El caso se clasifica como posible incidente de seguridad grave
2. Escalación al equipo CIRT.
3. Obtención conjunta de toda la información posible para mitigar la ofensa
4. Reuniones con dirección y otros departamentos para obtener ayuda y soporte en caso de actuación rápida (desactivar la salida a Internet, por ejemplo).
5. Un equipo mínimo monitoriza las actividades diarias para verificar que otros incidentes no se generan al mismo tiempo.

Escalación de un problema con los SIEM.

Si una de las reglas de monitorización del SOC fuera generada, el analista debe contactar con el equipo de ingeniería para solucionarlo lo antes posible.

1. El caso se clasifica como un posible problema de configuración/comunicación con los SIEM
2. Se recoge toda la información relevante del caso.
3. Escalación al equipo de ingeniería. En caso de que ocurra fuera del horario de oficina, se contactará con el ingeniero de guardia, informando a dirección.

Escalación a un departamento concreto (Reglas específicas)

En algunos casos específicos, según sea definido en el caso de uso (véase SOC-SOP-0001-Implementación de Casos de Uso (CU)), ciertos equipos deben ser contactados, ya que serán los que tienen la capacidad de actuar sobre la alerta. En este caso se debe enviar la información del caso a ellos, en lugar de ser escalados a través del SOC.

1. El caso se detecta y se confirma que debe ser enviado a otro departamento.
2. Se recoge toda la información relevante del caso.
3. Se contacta con el departamento interesado dependiendo del tipo de respuesta requerida.
4. En caso de que el departamento requiere soporte adicional del SOC, se procedería con la escalación genérica mencionada en este procedimiento.

Referencias

SOC-SOP-0006-Monitorización de alertas

SOC-SOP-0005-Plan de recuperación ante desastres (Disaster Recovery)

SOC-SOP-0008-Modificación y mejora de reglas SIEM

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	20 Mar 2020
Requerido por	ingeniería SOC, Analistas SOC, Fincomp, auditores
Fecha límite de activación	18 May 2020
Creador	Ingeniero SOC
Responsable	@ Daniel Rodríguez Fueyo
Última fecha de revisión	13 May 2020

Tabla de revisiones del documento

Versión actual del documento	1.0
Fecha de modificación	11 May 2020
Editor	Ingeniero SOC
Persona que ha aprobado los cambios	@ Daniel Rodríguez Fueyo
Última fecha de aprobación	13 May 2020

Introducción al procedimiento

En el momento en el que una regla es creada, no se mantiene estática permanentemente. Al ser la red de una empresa un entorno cambiante, ciertas modificaciones deben ser aplicadas a éstas para que sirvan correctamente con su propósito. Por ello, debe existir un procedimiento para poder realizar y documentar estos cambios correctamente.

Objetivo

- Indicación de los pasos a seguir para solicitar y realizar cambios en las reglas SIEM.

Activadores del procedimiento y afectados

Activadores	Departamento/Puesto	Descripción
Analistas SOC	SOC (Analistas)	Petición de una modificación en una regla
Ingenieros SOC	SOC (ingeniería)	Petición de una modificación en una regla
Afectados	**Departamento/Puesto**	**Descripción**
Ingenieros SOC	SOC (ingeniería)	Aplicación de la modificación de las reglas en los SIEM

Materiales requeridos

- Petición de cambio: Acceso analista a Qradar/Splunk.
- Ejecución del cambio: Acceso Administrador a Qradar/Splunk.

Desarrollo del procedimiento

Se dividirá el procedimiento en dos partes: una la correspondiente a la petición de un cambio en la regla, y la segunda parte, la que corresponde con la modificación de la regla en el SIEM.

Petición de cambio en una regla

Una vez que una regla sea identificada como susceptible del cambio, se debe rellenar una petición destinada a ingeniería con los cambios requeridos. Esta petición será verificada por los analistas senior antes de ser enviada, para comprobar que los requerimientos son posibles:

- **Nombre de la regla:** nombre de la regla a modificar
- **Caso de Uso relacionado:** Nombre del caso de uso del que deriva la regla
- **Entorno SIEM:** Qradar/Splunk
- **Ejemplo de ofensa:** el número de una ofensa donde se haya observado el posible cambio.
- **Cambio propuesto:** Descripción del cambio a realizar en la regla.
- **Razón del cambio:** confirmación de que el cambio puede ser posible, o explicación de cómo mejoraría la regla.
- **Prioridad:** Baja-media-alta. Inclusión de la prioridad., dependiendo de si el cambio es muy necesario para la regla, o puede esperar.

Ejecución de cambio en una regla

Una vez que la petición llega a ingeniería, se debe verificar que la reglar se puede modificar como se ha requerido, y que el cambio no influye en otras reglas.

1. **Si el cambio no es posible:** se debe informar de las razones a la persona que ha enviado la petición, una copia a dirección y cerrar el caso.
2. **Si el cambio es posible:** Ingeniería inserta las modificaciones requeridas en la regla del entorno de test, se deja bajo monitorización, y si la regla no genera anomalías, se aplica el cambio en producción.

⚠ Se debe documentar cada cambio de la regla en su correspondiente documento de descripción

Referencias

SOC-SOP-0002-Implementación y prueba de reglas en SIEM

SOC-SOP-0001-Implementación de Casos de Uso (CU)

SOC-SOP-0006-Monitorización de alertas

SOC-SOP-0005-Plan de recuperación ante desastres (Disaster Recovery)

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	20 Mar 2020
Requerido por	Auditores, Fincomp
Fecha límite de activación	18 May 2020
Creador	Ingeniería SOC, @ Daniel Rodríguez Fueyo
Responsable	@ Daniel Rodríguez Fueyo
Última fecha de revisión	06 May 2020

Tabla de revisiones del documento

Versión actual del documento	1.2
Fecha de modificación	04 May 2020
Editor	*Ingeniero SOC 1*
Persona que ha aprobado los cambios	@ Daniel Rodríguez Fueyo
Última fecha de aprobación	06 May 2020

Introducción al procedimiento

Aunque actualmente el objetivo del SOC será monitorizar la red de producción, y los colectores también están emplazados en ella, las soluciones SIEM no están incluidas por defecto en el plan general de recuperación de desastres de la compañía. Se ha pedido por parte de Fincomp que se cree un procedimiento paralelo al general para actuar en caso de una disrupción en el sistema.

El procedimiento siguiente enumera las medidas tomadas para evitar que se produzca cualquier evento que afecte a la disponibilidad de la monitorización, y de actuación en caso de que sea inevitable y deba ser mitigado en tiempo y forma.

Objetivo

- Indicación de los puntos aplicados para la consistencia de la disponibilidad en caso de un evento de fuerza mayor.
- Muestra de los pasos de recuperación y actuación en caso de desastre.

Activadores del procedimiento y afectados

En este procedimiento incluiremos los posibles activadores en este procedimiento, los cuales puede ser el propio SOC, o un departamento externo.

Activadores	Departamento/Puesto	Descripción
SOC	Analista	Acceso al SIEM no disponible
Externos	Departamento externo	Los reportes, notificaciones no llegan desde el SIEM
SOC	Ingeniería	Las notificaciones de servicios no disponibles llegan (heartbeats)
Redes	Departamento de redes	La red se encuentra caída y no hay conexión.
Seguridad física	Seguridad de la compañía	Se ha producido un evento inesperado y se deben abandonar las instalaciones.
Afectados	**Departamento/Puesto**	**Descripción**
SOC	Todos los puestos	El SOC no funciona correctamente, no se puede responder a las amenazas.

Materiales requeridos

- Acceso administrador a Qradar por SSH.
- Acceso administrador Splunk por SSH.
- Acceso vía VPN a la red de la empresa.
- (Opcional) acceso físico a los dispositivos (centro de datos).

Inclusión de mitigación en la red

Para mitigar con antelación posibles problemas en el acceso debido a la congestión en la red, se han tomado medidas en la implementación de cara a proteger la disponibilidad del sistema. Las medidas introducidas han sido las siguientes:

- Instalación de las consolas y colectores en un modelo de alta disponibilidad (high availability)

Todas las instalaciones de los dispositivos de monitorización y consolas SIEM han sido instalado en modalidad de alta disponibilidad, siguiendo un modelo activo pasivo. Este sistema permite que, en caso de que el dispositivo falle, el secundario tome el control hasta que el primario estuviera disponible y funcionara correctamente.

Este tipo de implementación es costosa (incrementa el doble el número de dispositivos), pero a la larga es muy útil, pudiendo reutilizar los dispositivos en otras zonas si fuera necesario sin tener que ampliar el presupuesto.

- Consolas y colectores instalados en un centro de datos redundante.

Los colectores principales tienen un equivalente conectado en un centro de datos que está situado geográficamente en otra población (diferente país), en caso de un desastre, el tráfico podría ser desviado a este centro temporalmente para continuar la monitorización.

- Implementación de casos de uso específicos para detectar caídas.

Un caso de uso se ha creado para monitorizar cuando los logs y eventos dejan de ser enviados a los SIEM, de esta forma se puede identificar rápidamente e informar al departamento correspondiente y a ingeniería del SOC para verificar el porqué de la situación.

- Monitorización 24 horas por parte de un equipo específico de la empresa.

Un equipo contratado por Fincomp monitoriza continuamente toda la infraestructura de red, identificando y contactando a las partes implicadas si algún dispositivo conectado presenta problemas.

Desarrollo del procedimiento

> Se procederá a realizar un desglose dependiendo del tipo de incidencia reportada y la respuesta, ya que puede haber grandes diferencias dependiendo del tipo de problema.

Acceso al SIEM no disponible

En caso de que se detecte que el SIEM no está disponible para monitorizar las ofensas, se deben seguir los siguientes pasos:

1. Recabar la información necesaria:
    a. Tiempo en el que se observó la incidencia.
    b. Si sigue activo
    c. Qué parte del servicio está inoperativa
    d. Si otras secciones de la red no están disponibles.
2. Escalar el incidente a ingeniería
    a. Si se produce fuera de horario de oficina, un ingeniero se encuentra de guardia para responder antes estos problemas. Contactar vía telefónica.

    b. Enviar un email con la información
3. Informar dirección del incidente

Reglas específicas no funcionan correctamente / eventos no llegan al SIEM

1. Recabar la información necesaria:
    a. Qué dispositivo no envía la información
    b. Cuántas reglas o eventos no llegan.
    c. Si el problema persiste.
    d. Si otras secciones de la red no están disponibles.
2. Contactar con ingeniería y el departamento responsable
    a. Enviar un email o contactar vía telefónica para intentar solventar el problema.
    b. Proporcionar los datos obtenidos.
3. Enviar un informe a dirección, por si otras acciones fueran necesarias.

Red se encuentra sin acceso

1. Comprobar si alguno de los accesos remotos a las máquinas funciona.
2. Contactar con el departamento de redes y comprobar si es un fallo general o específico.
3. Intentar reiniciar manualmente los sistemas si es posible.
4. En caso de no poder revertir la situación, contactar con el centro de datos secundario y activar el equipo de emergencia.
5. Enviar un informe a dirección.

Desastre en las oficinas y centro de datos (inaccesibles)

1. Comprobar si los sistemas son accesibles mediante VPN para analistas e ingeniería.
2. En caso negativo, contactar con el centro de datos secundario (si no se ha activado directamente) y ordenar activación del sistema secundario.
3. Mantener informada a dirección, en caso de que sean necesarias mayores decisiones.

Referencias

SOC-SOP-0006-Monitorización de alertas

SOC-SOP-0001-Implementación de Casos de Uso (CU)

SOC-SOP-0001-Implementación de Casos de Uso (CU)

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	20 Mar 2020
Requerido por	Fincomp, Auditores
Fecha límite de activación	12 Apr 2020
Creador	Service Delivery Manager, Ingenieros del SOC
Responsable	@ Daniel Rodríguez Fueyo
Última fecha de revisión	09 Apr 2020

Tabla de revisiones del documento

Versión actual del documento	1.1
Fecha de modificación	09 Apr 2020
Editor	Service Delivery Manager
Persona que ha aprobado los cambios	@ Daniel Rodríguez Fueyo
Última fecha de aprobación	09 Apr 2020

Introducción al procedimiento

Un caso de uso es un supuesto de actividad ocurrida tanto dentro de la organización como fuera de esta, pero que tiene repercusiones dentro de esta, pudiendo afectar de manera negativa la reputación o las finanzas de un modo inesperado. En el caso que ocupa al SOC, estas actividades tendrán relación con la seguridad informática de Fincomp. Estos casos de uso conllevan una respuesta al supuesto ¨riesgo¨, para poder hacerle frente, mitigando o eliminando el posible impacto.

El presente procedimiento describe cómo se debe actuar para la creación e implementación de un caso de uso, el cual será utilizado por la organización y el SOC propuesto.

Objetivo

- Identificar correctamente los puntos claves del caso y documentarlos correctamente.
- Poder extraer los datos relevantes para crear una regla o respuesta acorde de forma efectiva.
- Proveer de los pasos necesarios para la creación de múltiples casos de uso en el futuro.

Activadores del procedimiento y afectados

Los casos de uso pueden ser activados de múltiples formas, y pueden afectar a un rango muy amplio de la organización, dependiendo de la zona donde se generen, sistema afectado o departamento.

Este procedimiento no puede dar un activador u afectado específico, ya que engloba la creación de todos los casos de uso, pero se da una idea de cómo elaborar y encontrarlos.

Activadores	Departamento/Puesto	Descripción

SOC	Analista	Propuesta de caso a partir de búsqueda de logs.
Auditoría	Banco Central	Debido a regulación, un nuevo caso debe ser implementado.
Admin. Windows	Sistemas Windows	Se ha observado una posible puerta trasera en el sistema, un caso de uso debe ser creado para monitorear y mitigar en caso de que sea detectada.
Afectados	**Departamento/Puesto**	**Descripción**
Admin. Windows	Sistemas Windows	Se deben proveer con los eventos de las máquinas Windows que puedan estar afectadas por la vulnerabilidad
SOC	Analistas e Ingenieros	Crear la regla acorde al caso de uso y monitorizar.
Directorio activo	Departamento de Directorio activo y accesos (IAM)	Notificar mediante email si el caso de uso ha tenido resultado positivo (se ha activado), para observar lo que ha ocurrido y actuar de forma inmediata.

Materiales requeridos

Los materiales que se requerirán principalmente para el desarrollo del procedimiento son los eventos que se enviarán a los SIEM y se acuerdan en el caso de uso, para poder ejecutar la activación correctamente.

Se deberá indicar en cada caso de uso el tipo de fuente de logs necesaria para monitorizar el caso.

Desarrollo del procedimiento

1. Una vez identificados los activadores del caso u interesados, se debe realizar una reunión entre estos y el SDM para concretar los puntos principales y obtener los datos esenciales con los que generar el caso de uso. Estas reuniones deberían estar apoyadas por un miembro de ingeniería del SOC si fuera posible, ya que ayudaría a traducir el caso de forma técnica y ver si éste fuese posible de implementar. Se debe incluir en esta fase:

- El tipo de log requerido y si es posible enviarlo al SIEM en ese momento (la infraestructura lo alcanza).
- La prioridad del caso.
- El tipo de respuesta que se desea; ya sea una ofensa a monitorizar, un email a un departamento específico, o un reporte con los datos generados.

2. Una vez obtenidos los datos, se debe revisar con ingeniería (si no se ha hecho ya en el paso anterior) si con la información obtenida se puede proceder. En caso negativo se volvería al punto 1, para obtener más datos. En caso positivo, se seguiría adelante, teniendo en cuenta en este punto la prioridad y criticalidad de los sistemas y el caso en sí.

3. En este punto, Ingeniería debe traducir la información en un caso técnico, capaz de llevarse a cabo en el SIEM.

4. El caso se crea. se debe proceder ahora a crear la regla acorde en el SIEM, que se active cuando las condiciones sean las propuestas.

Referencias

SOC-SOP-0004-Creación y mantenimiento de Libros de reglas (Playbooks)

SOC-SOP-0006-Monitorización de alertas

SOC-SOP-0002-Implementación y prueba de reglas en SIEM

SOC-UC-0001-Intentos múltiples de autenticación fallidos

Tabla de estado del documento

Estado del documento	REQUERIDO	ACTIVO

Fecha creación	06 Apr 2020
Requerido por	Auditores, Fincomp, SOC
Fecha límite de activación	10 Apr 2020
Creador	Service Delivery Manager, Ingeniero SOC
Responsable	@ Daniel Rodríguez Fueyo
Última fecha de revisión	10 Apr 2020
Regla creada	SOC-RC-0001-Intentos múltiples de autenticación fallidos
Tipo de registro utilizado	Windows, Linux
Respuesta	ALERTA SIEM

Tabla de revisiones del documento

Versión actual del documento	1.0
Fecha de modificación	10 Apr 2020
Editor	Service Delivery Manager
Persona que ha aprobado los cambios	@ Daniel Rodríguez Fueyo
Última fecha de aprobación	10 Apr 2020

Alcance

El caso de uso cubre actualmente todos los dispositivos con sistema operativo Windows o Linux implementados en la red.

Objetivo

Identificar posibles intentos fraudulentos de acceso a las cuentas de usuario de la compañía, visualizando posibles ataques de fuerza bruta para acceder a la red.

Materiales requeridos

- Qradar.
- Splunk.
- Dispositivos Windows o Linux para monitorizar.

Condiciones

Los dispositivos para monitorizar serán Windows y Linux.

La actividad será local, no hay IPs públicas en este caso.

En caso de que una cuenta falle la contraseña en más de 10 ocasiones, deberá generar una alerta para informar al SOC e investigar el contexto.

Respuesta

Creación de una alerta en los SIEM (Qradar y Splunk).

Referencias

SOC-SOP-0001-Implementación de Casos de Uso (CU)

SOC-PC-0001-Intentos múltiples de autenticación fallidos

SOC-UC-0002-Comandos sospechosos ejecutados

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	13 Apr 2020
Requerido por	Persona, entidad o grupo que ha pedido/necesita el documento
Fecha límite de activación	17 Apr 2020
Creador	Service Delivery Manager, Ingeniero SOC
Responsable	@ Daniel Rodríguez Fueyo
Última fecha de revisión	17 Apr 2020
Regla creada	SOC-RC-0002-Comandos sospechosos ejecutados
Tipo de registro utilizado	Máquinas Windows
Respuesta	ALERTA SIEM

Tabla de revisiones del documento

Versión actual del documento	1.0
Fecha de modificación	15 Apr 2020
Editor	Ingeniero SOC
Persona que ha aprobado los cambios	@ Daniel Rodríguez Fueyo
Última fecha de aprobación	17 Apr 2020

Alcance

El alcance comprende todas las máquinas Windows de la red de la empresa.

Objetivo

Detectar un posible movimiento lateral de un usuario comprometido a otras zonas de la red.

Materiales requeridos

- Qradar.
- Splunk.
- Dispositivo/s Windows desde donde se envían los eventos.

Condiciones

El contexto es local, pero la actividad podría venir desde el exterior.

Una vez se ejecuten 4 comandos distintos que puedan indicar un movimiento lateral, en un plazo de 1 hora, la alerta debería generarse.

Los comandos serán proporcionados por ingeniería en la regla correspondiente.

Respuesta

Creación de una alerta en los SIEM. Escalación en caso de posible incidente de seguridad.

Referencias

SOC-SOP-0001-Implementación de Casos de Uso (CU)

SOC-PC-0002-Comandos sospechosos ejecutados

SOC-UC-0003-Eventos no llegan desde endpoints

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	20 Apr 2020
Requerido por	SOC, Fincomp, auditores.
Fecha límite de activación	24 Apr 2020
Creador	Service Delivery Manager, Departamento de riesgos de la empresa
Responsable	@ Daniel Rodríguez Fueyo
Última fecha de revisión	24 Apr 2020
Regla creada	SOC-RC-0003-Eventos no llegan desde endpoints
Tipo de registro utilizado	Windows, Linux
Respuesta	ALERTA SIEM EMAIL

Tabla de revisiones del documento

Versión actual del documento	1.2
Fecha de modificación	23 Apr 2020
Editor	Ingeniero SOC
Persona que ha aprobado los cambios	@ Daniel Rodríguez Fueyo
Última fecha de aprobación	24 Apr 2020

Alcance

El alcance cubre los equipos bajo Windows y Linux

Objetivo

El objetivo de este caso de uso es el de detectar si uno de los dispositivos endpoints (Windows o Linux) deja de enviar eventos al SIEM.

Materiales requeridos

- Qradar.
- Splunk.

- Dispositivo/s Windows o Linux desde donde se dejan de enviar los eventos (logs)

Condiciones

En este caso el contexto es del dispositivo en sí, por lo que es tráfico local.

Cuando, desde un tiempo específico los eventos no llegan al SIEM, una alerta debe ser generada para informar de este problema.

Respuesta

Creación de una alerta en los SIEM. Escalación en caso de posible incidente de seguridad.

Envío de un correo electrónico al equipo de redes de la empresa, para responder de forma rápida en caso de un incidente real.

Referencias

SOC-SOP-0001-Implementación de Casos de Uso (CU)

SOC-PC-0003-Eventos no llegan desde endpoints

SOC-UC-0004-Posible escáner de red detectado (Local-Local)

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	27 Apr 2020
Requerido por	SOC, Fincomp, auditores
Fecha límite de activación	01 May 2020
Creador	Ingeniero SOC
Responsable	@ Daniel Rodríguez Fueyo
Última fecha de revisión	30 Apr 2020
Regla creada	SOC-RC-0004-Posible escáner de red detectado (Local-Local)
Tipo de registro utilizado	Cualquier dispositivo de la red
Respuesta	ALERTA SIEM EMAIL

Tabla de revisiones del documento

Versión actual del documento	1.0
Fecha de modificación	26 Apr 2020
Editor	Service Delivery Manager
Persona que ha aprobado los cambios	@ Daniel Rodríguez Fueyo
Última fecha de aprobación	30 Apr 2020

Alcance

El alcance de este caso de uso se extiende a cualquier dispositivo implantado en la red susceptible de ser alcanzado por un escaneo de puertos.

Objetivo

Detectar si se está realizando un escaneo a un dispositivo concreto, puede corresponder a la fase de reconocimiento previa a un ataque a la red o un intento de acceso.

Materiales requeridos

- Qradar.
- Splunk.
- Dispositivo/s objetivo que envía eventos a los SIEM.

Condiciones

El contexto de escáner deberá ser para este caso local. Tanto origen como destino tendrán asignada una IP privada.

Respuesta

Creación de una alerta en los SIEM gestionada por el SOC.

Envío de un email al equipo de vulnerabilidades para descartar que pudiera tratarse de un escáner de la propia empresa.

Referencias

SOC-SOP-0001-Implementación de Casos de Uso (CU)

SOC-PC-0004-Posible escáner de red detectado (Local-Local)

SOC-UC-0005- Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	04 May 2020
Requerido por	SOC, Fincomp, auditores
Fecha límite de activación	08 May 2020
Creador	Service Delivery Manager
Responsable	@ Daniel Rodríguez Fueyo
Última fecha de revisión	07 May 2020
Regla creada	SOC-RC-0005-Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)
Tipo de registro utilizado	Eventos de la máquina con conexión a Internet: Proxy, el propio dispositivo, SSL VPN)
Respuesta	ALERTA SIEM

Tabla de revisiones del documento

Versión actual del documento	1.0
Fecha de modificación	06 May 2020
Editor	Ingeniero SOC
Persona que ha aprobado los cambios	@ Daniel Rodríguez Fueyo
Última fecha de aprobación	08 May 2020

Alcance

El alcance del caso concierne a todos los dispositivos con conexión a Internet.

Objetivo

Detectar una conexión a una página con reputación baja, lo que puede indicar que se puede tratar de una actividad sospechosa, como botnet, phishing, malware…

Materiales requeridos

- Qradar.
- Splunk.
- Lista o feeder con la reputación de las páginas web a las que se accede.

Condiciones

Si el evento generado en un dispositivo en la red posee como IP de origen o destino una IP catalogada como blacklisted, el caso deberá activarse. La condición intrínseca es que la conexión será Local a remoto o viceversa.

Respuesta

Se generará una alerta en los SIEM para verificar si el acceso entraña riesgo o la página en realidad no presenta problemas.

Referencias

SOC-SOP-0001-Implementación de Casos de Uso (CU)

SOC-PC-0005-Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)

SOC-SOP-0002-Implementación y prueba de reglas en SIEM

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	20 Mar 2020
Requerido por	Fincomp, auditores
Fecha límite de activación	12 Apr 2020
Creador	Ingenieros del SOC
Responsable	@ Daniel Rodríguez Fueyo
Última fecha de revisión	08 Apr 2020

Tabla de revisiones del documento

Versión actual del documento	1.0
Fecha de modificación	07 Apr 2020
Editor	Ingeniero N1
Persona que ha aprobado los cambios	@ Daniel Rodríguez Fueyo
Última fecha de aprobación	08 Apr 2020

Introducción al procedimiento

Una vez que el caso de uso está definido de forma técnica, se puede implementar su regla correspondiente en la solución SIEM específica que se ha elegido. Este procedimiento enseña a centrarse en encontrar los puntos más importantes, para facilitar y estandarizar la forma en la que se crean reglas. De este modo, el proceso podrá ser exportado o utilizado por FinComp si fuera necesario.

Objetivo

Creación de las reglas en las soluciones SIEM de forma correcta.

Estructuración correcta y consistencia en la creación de reglas.

Materiales requeridos

- *Eventos obtenidos de los sistemas requeridos para cada regla (log sources) e insertados en el SIEM mediante colectores.*
- Acceso de administrador a Qradar.
- Acceso de administrador a Splunk.

Desarrollo del procedimiento

1. Obtener mediante SOC-SOP-0001-Implementación de Casos de Uso (CU), el caso de uso específico y la información requerida para implementar la regla.
2. Ingeniería crea los puntos básicos para crear la regla correctamente, los cuales son:
    a. El tipo de respuesta. Ya sea creando una ofensa en el SIEM, u otro tipo de acción.

b. Cuál es el parámetro que hace saltar la regla. Este parámetro es el decisivo a la hora de organizar las ofensas. Si, por ejemplo, el parámetro objetivo de una regla es el usuario, la respuesta estará enfocada en el usuario; si hubiera dos usuarios activando la regla, se generarán dos ofensas distintas.
c. La fuente de los eventos específica: donde se produce la actividad. Windows, linux, AD, Proxies …
d. El límite para implementar que la regla se active: En este caso puede ser que una sola acción no sea necesaria. Como ejemplo se puede indicar que una ofensa se genere si el mismo usuario falla la contraseña 5 veces en 15 minutos.
e. Las exclusiones a la regla: Puede ser que algunos parámetros sean aceptados en la regla, y debe ser indicado, ya que el no hacerlo haría generar falsos positivos en el sistema.

3. Se implementa con código puro o con el asistente la regla, incluyendo los parámetros indicados anteriormente.
4. Una vez finalizada la regla, se debe probar (en entorno controlado) y ver si es efectiva. En este punto todavía no se debe generar una respuesta, sino que se monitoriza desde ingeniería.
5. Se crearía el libro de reglas específico para la regla. Véase SOC-SOP-0004-Creación y mantenimiento de Libros de reglas (Playbooks) .
6. Una vez el playbook sea efectivo, la regla pasa a funcionar de manera activa.
7. Si se observaran problemas en el momento en que la regla sea funcional, ésta se desactivaría y se revisaría. Véase SOC-SOP- 0008-Modificación y mejora de reglas SIEM para más información.

Referencias

SOC-SOP-0001-Implementación de Casos de Uso (CU)

SOC-SOP-0008-Modificación y mejora de reglas SIEM

SOC-SOP-0004-Creación y mantenimiento de Libros de reglas (Playbooks)

SOC-SOP-0008-Modificación y mejora de reglas SIEM

SOC-RC-0001-Intentos múltiples de autenticación fallidos

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	13 Apr 2020
Requerido por	SOC, Fincomp, auditores
Fecha límite de activación	17 Apr 2020
Creador	Ingeniero SOC
Responsable	@ Daniel Rodriguez Fueyo
Última fecha de revisión	17 Apr 2020
Caso de uso relacionado	SOC-UC-0001-Intentos múltiples de autenticación fallidos
Tipo de registro utilizado	Windows, Linux
Respuesta	ALERTA SIEM

Descripción

Esta regla Identifica posibles intentos fraudulentos de acceso a las cuentas de usuario de la compañía, visualizando posibles ataques de fuerza bruta para acceder a la red.

Bloques utilizados

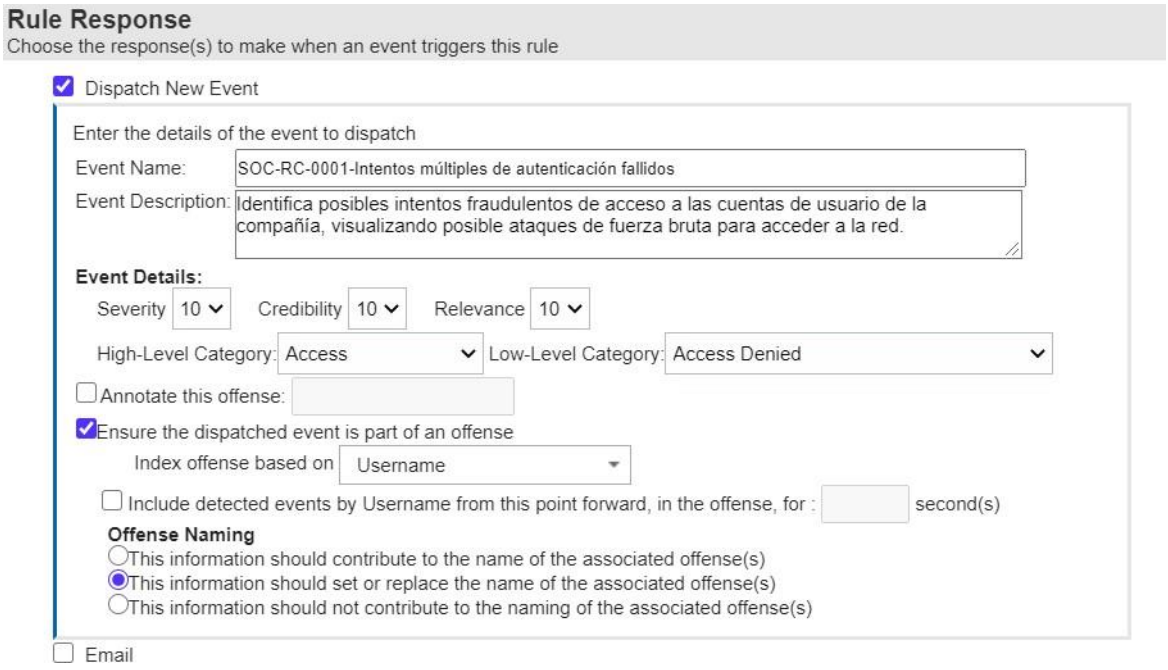
Los bloques utilizados son los siguientes:

BB: CategoryDefinition: Authentication Failures: Indica los eventos tanto para Linux como para Windows en los que se muestre que una cuenta ha fallado la autenticación

Código de la regla

Respuesta

Creación de una alerta en los SIEM (Qradar y Splunk).



Referencias

SOC-SOP-0002-Implementación y prueba de reglas en SIEM

SOC-SOP-0008-Modificación y mejora de reglas SIEM

SOC-PC-0001-Intentos múltiples de autenticación fallidos

SOC-RC-0002-Comandos sospechosos ejecutados

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	20 Apr 2020

Requerido por	SOC, Fincomp, auditores
Fecha límite de activación	24 Apr 2020
Creador	Ingeniero SOC
Responsable	@ Daniel Rodriguez Fueyo
Última fecha de revisión	24 Apr 2020
Caso de uso relacionado	SOC-UC-0002-Comandos sospechosos ejecutados
Tipo de registro utilizado	Máquinas Windows
Respuesta	ALERTA SIEM

Descripción

Esta regla detecta un posible movimiento lateral de un usuario comprometido a otras zonas de la red.

Bloques utilizados

El bloque principal en este caso es un Reference Set creado por Ingeniería, denominado *Comandos sospechosos*

Value	Origin
whoami.exe	daniel
cmd.exe	daniel
nslookup.exe	daniel
reg.exe	daniel
svchost.exe	daniel
HOSTNAME.EXE	daniel
ipconfig.exe	daniel

Código de la regla

Test definitions

AND when the event(s) were detected by one or more of **Kali Linux Red Team, WindowsAuthServer @ MSEDGEWIN10**

AND when an event matches **any** of the following **Context is Local to Local**

AND when **any** of **Process Name (custom)** are contained in **any** of **Comandos sospechosos - AlphaNumeric**

AND when at least **4** events are seen with the same **Process Name (custom)** in **15 minutes**

Respuesta

creación de una alerta en los SIEM. Escalación en caso de posible incidente de seguridad.

Referencias

SOC-SOP-0002-Implementación y prueba de reglas en SIEM

SOC-SOP-0008-Modificación y mejora de reglas SIEM

SOC-PC-0002-Comandos sospechosos ejecutados

SOC-RC-0003-Eventos no llegan desde endpoints

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	27 Apr 2020
Requerido por	SOC, Fincomp, auditores
Fecha límite de activación	01 May 2020
Creador	Ingeniero SOC
Responsable	@ Daniel Rodriguez Fueyo
Última fecha de revisión	01 May 2020
Caso de uso relacionado	SOC-UC-0003-Eventos no llegan desde endpoints
Tipo de registro utilizado	Windows, linux
Respuesta	ALERTA SIEM EMAIL

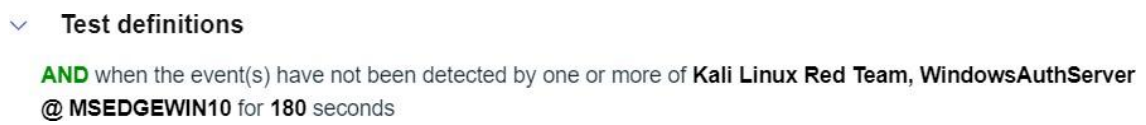
Descripción

Esta regla detecta si uno de los dispositivos endpoints (Windows o Linux) deja de enviar eventos al SIEM.

Bloques utilizados

No hay bloques específicos utilizados, los eventos en este caso NO existen.

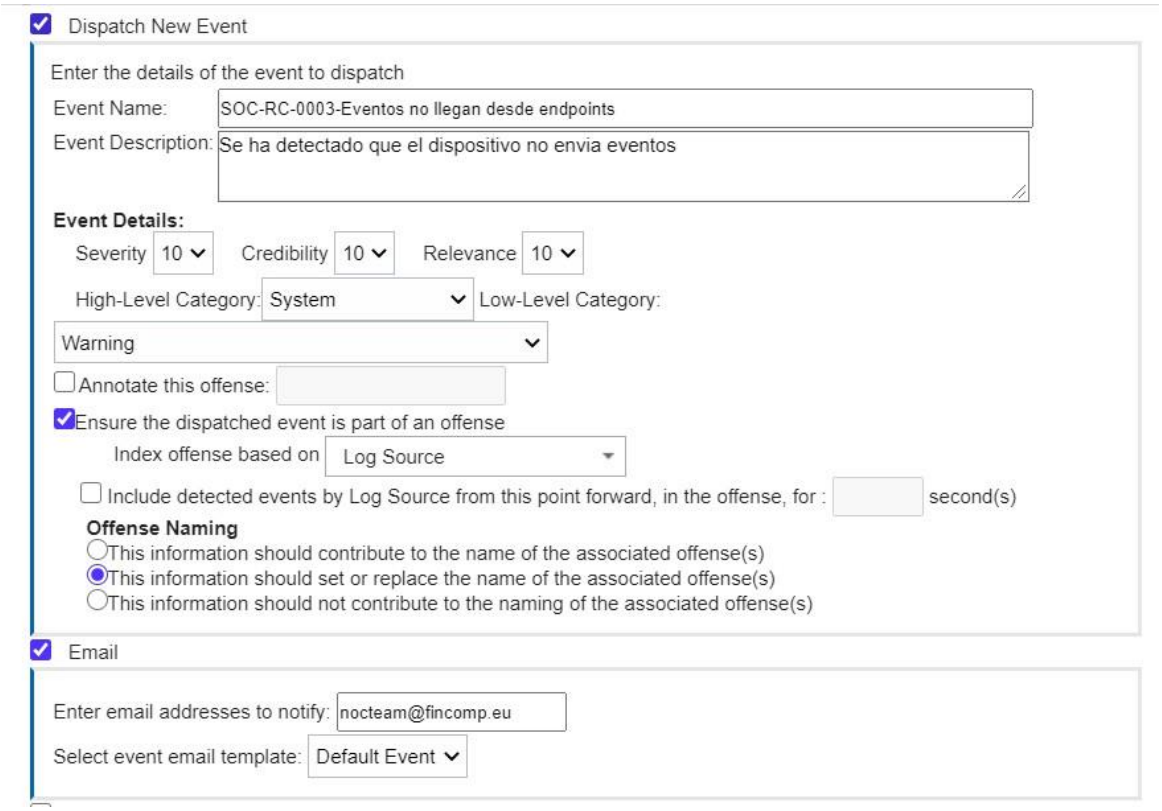
Código de la regla



Respuesta

Creación de una alerta en los SIEM. Escalación en caso de posible incidente de seguridad.

Envío de un correo electrónico al equipo de Riesgo de la empresa, para responder de forma rápida en caso de un incidente real.



Referencias

SOC-SOP-0002-Implementación y prueba de reglas en SIEM

SOC-SOP-0008-Modificación y mejora de reglas SIEM

SOC-PC-0003-Eventos no llegan desde endpoints

SOC-RC-0004-Posible escáner de red detectado (Local-Local)

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	04 May 2020
Requerido por	SOC, Fincomp, auditores
Fecha límite de activación	08 May 2020
Creador	Ingeniero SOC
Responsable	@ Daniel Rodriguez Fueyo
Última fecha de revisión	08 May 2020
Caso de uso relacionado	SOC-UC-0004-Posible escáner de red detectado (Local-Local)
Tipo de registro utilizado	Cualquier dispositivo de la red
Respuesta	ALERTA SIEM EMAIL

Descripción

Esta regla detecta si se está realizando un escaneo a un dispositivo concreto, puede corresponder a la fase de reconocimiento previa a un ataque a la red o un intento de acceso.

Bloques utilizados

El bloque utilizado en este caso es el siguiente:

BB:CategoryDefinition: Firewall or ACL Denies, Excessive Firewall Denies from Local Host: Este bloque detecta eventos especiales que han sido denegados por el Firewall del dispositivo objetivo en varios puertos distintos.

Código de la regla

Test definitions

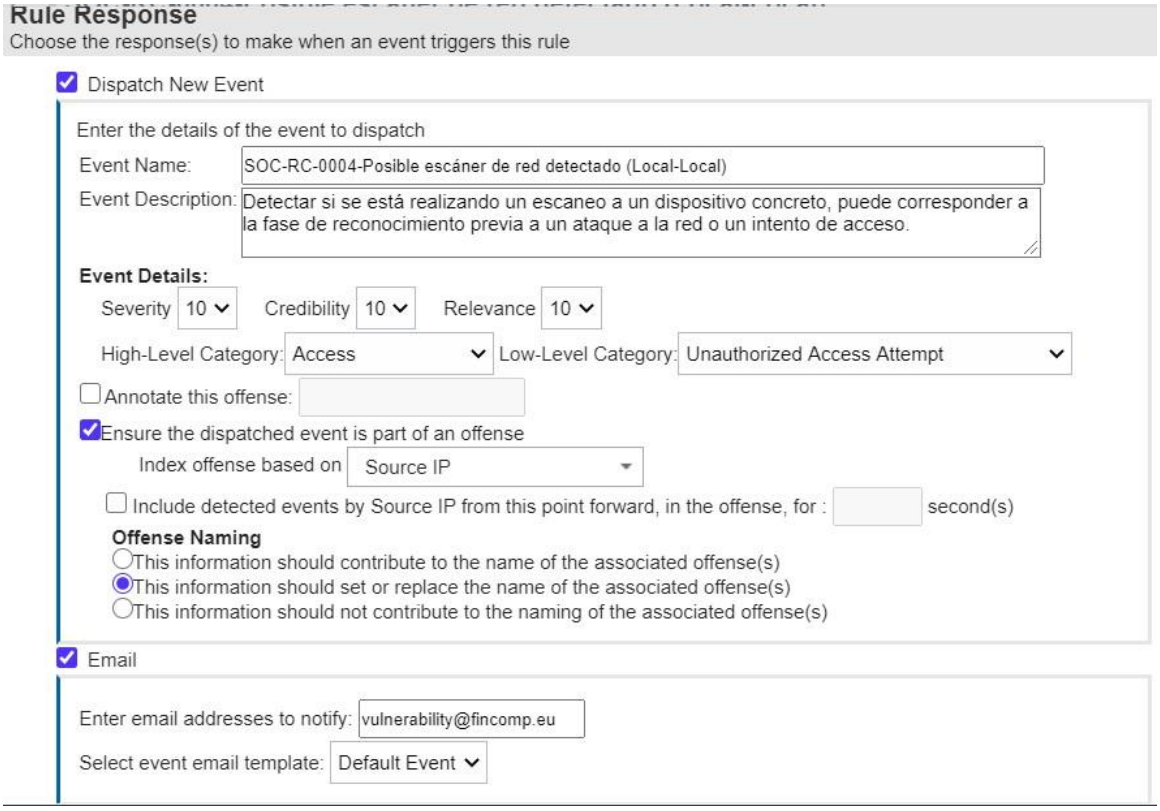
AND when the event(s) were detected by one or more of **Kali Linux Red Team, WindowsAuthServer @ MSEDGEWIN10**

AND when any of these **BB:CategoryDefinition: Firewall or ACL Denies, Excessive Firewall Denies from Local Host** with the same **source IP** more than **500** times, across **exactly 1 destination IP** within **5 minutes**

Respuesta

Creación de una alerta en los SIEM gestionada por el SOC.

Envío de un email al equipo de vulnerabilidades para descartar que pudiera tratarse de un escáner de la propia empresa.



Referencias

SOC-SOP-0002-Implementación y prueba de reglas en SIEM

SOC-SOP-0008-Modificación y mejora de reglas SIEM

SOC-PC-0004-Posible escáner de red detectado (Local-Local)

SOC-RC-0005-Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	11 May 2020
Requerido por	SOC, Fincomp, auditores
Fecha límite de activación	15 May 2020
Creador	Ingeniero SOC
Responsable	@ Daniel Rodriguez Fueyo
Última fecha de revisión	15 May 2020
Caso de uso relacionado	SOC-UC-0005- Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)
Tipo de registro utilizado	Eventos de la máquina con conexión a Internet: Proxy, el propio dispositivo, SSL VPN)
Respuesta	ALERTA SIEM

Descripción

Detecta una conexión a una página con reputación baja, lo que puede indicar que se puede tratar de una actividad sospechosa, como botnet, phishing, malware…

Bloques utilizados

En este caso se ha utilizado un Reference set para las direcciones IP de páginas con mala reputación, el nombre de la lista es *Paginas sospechosas*

Value	Origin
50.17.247.9	daniel
204.236.236.127	daniel
52.31.48.193	daniel
34.218.19.24	daniel
18.236.7.30	daniel
107.20.175.192	daniel
91.198.174.194	daniel
46.137.171.215	daniel
34.252.74.1	daniel
213.73.40.242	daniel

Código de la regla

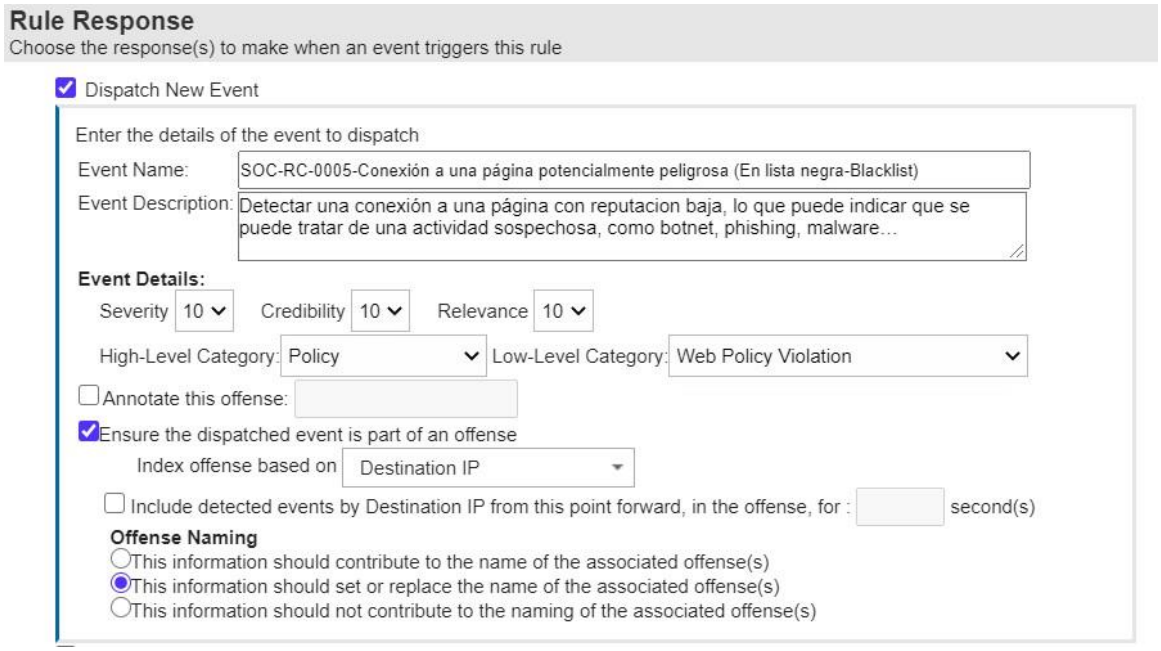
Test definitions

AND when **any** of **Destination IP** are contained in **any** of **Paginas sospechosas - IP**

AND when the event(s) were detected by one or more of **Kali Linux Red Team, WindowsAuthServer @ MSEDGEWIN10**

Respuesta

Se generará una alerta en los SIEM para verificar si el acceso entraña riesgo o la página en



Referencias

SOC-SOP-0002-Implementación y prueba de reglas en SIEM

SOC-SOP-0008-Modificación y mejora de reglas SIEM

SOC-PC-0005-Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)

SOC-SOP-0004-Creación y mantenimiento de Libros de reglas (Playbooks)

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	20 Apr 2020
Requerido por	Analistas SOC, @ Daniel Rodríguez Fueyo, SOC ingeniería, auditores, Fincomp
Fecha límite de activación	12 Apr 2020
Creador	Analistas Senior SOC
Responsable	@ Daniel Rodríguez Fueyo
Última fecha de revisión	09 Apr 2020

Tabla de revisiones del documento

Versión actual del documento	1.3
Fecha de modificación	06 Apr 2020
Editor	*Analista Senior 1*
Persona que ha aprobado los cambios	@ Daniel Rodríguez Fueyo
Última fecha de aprobación	09 Apr 2020

Introducción al procedimiento

Debido al amplio espectro de tecnologías que un SOC debe cubrir en su monitorización día a día (reverse proxy, proxies, DNS, linux, Windows, Cisco…), se debe incluir en la documentación del SOC una serie de consejos y pasos para poder analizar cada una de las diferentes alertas que las reglas implementadas en los SIEM generen. Gracias a estos libros de reglas o ¨Playbooks¨ los analistas podrán reducir el tiempo de análisis de las ofensas, actuando en su mitigación o escalación de una forma más efectiva y rápida.

> La activación de una regla en producción debe estar supeditada a que su correspondiente libro de reglas esté operativo y validado. En caso contrario la regla no podrá ser activada en producción.

Objetivo

- Indicación de los pasos concretos para la creación de Playbooks.
- Indicación de la estructura concreta para crear playbooks.

Materiales requeridos

- Acceso de editor a Confluence.
- Acceso a las documentaciones de las reglas y casos de uso.
- Acceso a Qradar.
- Acceso a Splunk.

Desarrollo del procedimiento

Una vez que se ha creado la regla correspondiente a la que se va a asignar el playbook (véase SOC-SOP-0002-Implementación y prueba de reglas en SIEM para más detalles) podremos proceder a:

Obtención general de los pasos

> ⚠ Esta parte del procedimiento debe ser realizada por un analista senior o un miembro de ingeniería.

En la fase inicial del procedimiento, se recabarán todos los pasos para poder completar la ofensa y cerrarla o escalarla convenientemente según corresponda. En este punto es necesario que, alguien con la experiencia en la tecnología que cubre el caso, lo realice.

Desglose de los pasos en subtareas

Una vez que toda la información del libro se ha obtenido, el analista debe intentar dividir las tareas en unidades mínimas, las cuales contendrían un paso específico para completar el libro.

Ejemplo de una tarea: Verificar la IP externa.

Completar las subtareas con información adicional

Ahora que todas las subtareas están creadas, deben completarse con la información necesaria que el analista debe aportar para completar la tarea, esta información adicional se completará con enlaces a otras secciones donde se desglosa la información.

Este procedimiento se realiza así para preparar el libro enfocado a todos los niveles de analista, tanto senior como junior, el senior simplemente verificará lo que hay que hacer; el junior podrá navegar en la descripción minuciosa de la tarea si tiene dudas de cómo resolverla.

Insertar y revisar las subtareas en el libro

Cuando las subtareas se hayan completado, otro analista senior o ingeniero deberá revisar si las tareas cumplen su propósito y se han incluido las necesarias para completar el análisis de principio a fin. En caso afirmativo, el playbook se puede activar, activando con ello la regla.

Prueba de la regla junto con el libro

Los analistas verifican que el libro ayuda a completar la ofensa. En caso de que se detecten tareas que puedan ser incluidas y algunas con errores, el libro deberá ser revisado y verificado una vez más por un analista senior.

Referencias

SOC-SOP-0002-Implementación y prueba de reglas en SIEM

SOC-SOP-0006-Monitorización de alertas

SOC-SOP-0007-Escalación de posibles incidentes de seguridad

SOC-SOP-0008-Modificación y mejora de reglas SIEM

SOC-PC-0001-Intentos múltiples de autenticación fallidos

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	20 Apr 2020
Creador	Analista SOC Senior
Responsable	@ Daniel Rodríguez Fueyo ,Ingeniero SOC
Última fecha de revisión	24 Apr 2020

Regla creada	SOC-RC-0001-Intentos múltiples de autenticación fallidos
Caso de uso relacionado	SOC-UC-0001-Intentos múltiples de autenticación fallidos

Descripción

Este Playbook ayuda al analista a verificar las alertas relacionadas con la regla SOC-RC-0001-Intentos múltiples de autenticación fallidos

- Asigna la ofensa a tu cuenta de usuario en el SIEM
- Verifica las ofensas relacionadas, puede ser que el mismo comportamiento haya sido visto antes y verificado

Pasos específicos de análisis

- Verifica la fuente de Logs, y si coincide con la dirección IP de origen.
- Verifica la IP de destino.
- Comprueba el número de intentos fallidos, ¿Puede corresponderse con un fallo humano?
- Busca el usuario en la alerta
- Busca el usuario en la base de datos y añádelos en la alerta.
- Verificar los eventos generados por el usuario y la IP durante el tiempo previo y consecuente, para verificar si no hay otra actividad sospechosa realizada.

⚠ Si en este caso se considera que el usuario ha fallado la autenticación de forma no intencionada, se puede contactar con el usuario directamente para verificación. En caso contrario la actividad debe ser escalada al equipo de respuesta y no alertar al usuario.

- Anota toda la información en la alerta mediante una nota.
- Rellena la información relativa a la conclusión del caso.
- Dependiendo del análisis:
  - Cierra el caso.
  - Escálalo según corresponda.

SOC-PC-0002-Comandos sospechosos ejecutados

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	27 Apr 2020
Creador	Analista SOC Senior
Responsable	@ Daniel Rodríguez Fueyo ,Ingeniero SOC
Última fecha de revisión	01 May 2020
Regla creada	SOC-RC-0002-Comandos sospechosos ejecutados
Caso de uso relacionado	SOC-UC-0002-Comandos sospechosos ejecutados

Descripción

Este Playbook ayudará al analista a verificar si la alerta relacionada con la regla SOC-RC-0002-Comandos sospechosos ejecutados es en realidad un movimiento lateral o no.

- Asigna la ofensa a tu cuenta de usuario en el SIEM
- Verifica las ofensas relacionadas, puede ser que el mismo comportamiento haya sido visto antes y verificado

Pasos específicos de análisis

- Verificar los comandos ejecutados que se han agregado a la alerta.
- Verificar el resto de los comandos ejecutados antes y después.
- Comprobar desde dónde han sido llamados los comandos: línea de comandos, conexión remota, a través de otro programa.
- Encontrar el usuario en la alerta y cotejar con la base de datos: *¿Es un usuario con conocimientos técnicos?

⚠ *Si el usuario no es técnico, puede ser una indicación de que la cuenta está comprometida, no se debe contactar en este caso.

- Verificar si existe alguna incidencia abierta que pueda requerir en ese tiempo la ejecución de esos comandos.
- Contactar con el usuario para verificar por qué ha realizado los comandos detectados**

✓ **Si existe un ticket y el usuario está relacionado con el equipo, puede ser contactado directamente

- Anota toda la información en la alerta mediante una nota.
- Rellena la información relativa a la conclusión del caso.
- Dependiendo del análisis:
    - Cierra el caso.
    - Escálalo según corresponda.

SOC-PC-0003-Eventos no llegan desde endpoints

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	04 May 2020
Creador	Analista SOC Senior
Responsable	@ Daniel Rodríguez Fueyo ,Ingeniero SOC
Última fecha de revisión	08 May 2020
Regla creada	SOC-RC-0003-Eventos no llegan desde endpoints
Caso de uso relacionado	SOC-UC-0003-Eventos no llegan desde endpoints

Descripción

Este libro de reglas permitirá al analista intentar verificar la alerta generada a partir de la regla SOC-RC-0003-Eventos no llegan desde endpoints

- Asigna la ofensa a tu cuenta de usuario en el SIEM
- Verifica las ofensas relacionadas, puede ser que el mismo comportamiento haya sido visto antes y verificado

Pasos específicos de análisis

- Verificación del Log source que no envía eventos.
- Verificación del sistema de alertas para comprobar que no hay ningún incidente en curso que pueda dar lugar a que no lleguen las alertas.
- Comprobación de los últimos logs antes de la caída, para descartar posible actividad maliciosa en el dispositivo.
    - Anota toda la información en la alerta mediante una nota.
    - Rellena la información relativa a la conclusión del caso.
    - Dependiendo del análisis:
        - Cierra el caso.
        - Escálalo según corresponda.

SOC-PC-0004-Posible escáner de red detectado (Local-Local)

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	11 May 2020
Creador	Analista SOC Senior
Responsable	@ Daniel Rodríguez Fueyo ,Ingeniero SOC
Última fecha de revisión	15 May 2020
Regla creada	SOC-RC-0004-Posible escáner de red detectado (Local-Local)
Caso de uso relacionado	SOC-UC-0004-Posible escáner de red detectado (Local-Local)

Descripción

El siguiente Playbook guiará al analista para verificar la información generada en la alerta relacionada con la regla SOC-RC-0004-Posible escáner de red detectado (Local-Local) y comprobar si el escaneo de la red es legítimo o es una actividad ajena a la empresa.

- Asigna la ofensa a tu cuenta de usuario en el SIEM
- Verifica las ofensas relacionadas, puede ser que el mismo comportamiento haya sido visto antes y verificado

Pasos específicos de análisis

- Verificación de la dirección de origen.
- Verificación de la dirección de destino.
- Comprobación de si la actividad sigue en curso.
- Búsqueda de todos los eventos relacionados con la posible IP atacante, para descartar que haya podido ser infectada.
- Comprobación de la lista de dispositivos de escaneo de la red legítimos, por si la regla ha generado un falso positivo.
- Si el equipo de vulnerabilidades no ha contestado, contactar con ellos para verificar que no sea un nuevo dispositivo o una prueba en progreso.
- Comprobar si existen eventos positivos de respuesta, o todos los intentos han sido bloqueados con éxito.
    - Anota toda la información en la alerta mediante una nota.
    - Rellena la información relativa a la conclusión del caso.
    - Dependiendo del análisis:
        - Cierra el caso.
        - Escálalo según corresponda.

SOC-PC-0005-Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	18 May 2020
Creador	Analista SOC Senior

Responsable	@ Daniel Rodríguez Fueyo ,Ingeniero SOC
Última fecha de revisión	22 May 2020
Regla creada	SOC-RC-0005-Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)
Caso de uso relacionado	SOC-UC-0005- Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)

Descripción

El presente PLaybook ayudará al analista a verificar si la conexión a la página web detectada por la regla SOC-RC-0005-Conexión a una página potencialmente peligrosa (En lista negra-Blacklist) es una actividad potencialmente peligrosa o puede descartarse.

- Asigna la ofensa a tu cuenta de usuario en el SIEM
- Verifica las ofensas relacionadas, puede ser que el mismo comportamiento haya sido visto antes y verificado

Pasos específicos de análisis

- Verificación de la IP de origen, que tipo de dispositivo de trata (endpoint, servidor, producción)
- Verificación de la IP de destino: reputación
- Comprobación del usuario.
- Tiempo de acceso a la página: ha sido durante horas de trabajo on en un horario extraño.
- Búsqueda de otra actividad realizada por el usuario.
- Comprobación de otras conexiones a la IP de destino. ¿Existe algún envío de información o comunicaciones frecuentes?
- Contactar a usuario para verificar el porqué del acceso (si no se sospecha una intención maliciosa).
    - Anota toda la información en la alerta mediante una nota.
    - Rellena la información relativa a la conclusión del caso.
    - Dependiendo del análisis:
        - Cierra el caso.
        - Escálalo según corresponda.

SOC-SOP-0003-Entrenamiento para analistas

Tabla de estado del documento

Estado del documento	REQUERIDO ACTIVO
Fecha creación	20 Mar 2020
Requerido por	SOC, auditores, Fincomp
Fecha límite de activación	10 May 2020
Creador	@ Daniel Rodríguez Fueyo
Responsable	@ Daniel Rodríguez Fueyo
Última fecha de revisión	08 May 2020

Tabla de revisiones del documento

Versión actual del documento	1.2
Fecha de modificación	06 Apr 2020
Editor	@ Daniel Rodríguez Fueyo
Persona que ha aprobado los cambios	@ Daniel Rodríguez Fueyo
Última fecha de aprobación	08 May 2020

Introducción al procedimiento

Incluso con la obtención de poderosas herramienta SIEM como pueden ser Qradar y Splunk, no se debe subestimar la creación de un plan para que los analistas posean el conocimiento necesario para trabajar con éstas. Sin un conocimiento correcto de la herramienta, la información obtenida puede ser incorrecta o se pueden omitir datos importantes para una que una investigación finalice correctamente.

En este Procedimiento se explicarán los tiempos, herramientas y procesos requeridos para que un analista pueda realizar una correcta labor de identificación, análisis y escalación de las alertas generadas en las herramientas SIEM. El proceso puede ser extrapolado a otras herramientas aparte de Qradar y Splunk, ya que la metodología de análisis de alertas es muy parecida, independientemente de la solución de monitorización empleada.

Objetivo

- Obtención de un plan por fases de entrenamiento para los nuevos analistas del SOC.
- Prueba del conocimiento y aptitud mediante pruebas en entornos de test.

Materiales requeridos

- Acceso de analista a Qradar
- Acceso de Analista a Splunk

Desarrollo del procedimiento

Se ha calculado que como mínimo, desde el momento en el que los nuevos analistas comienzan en su puesto de trabajo, un total de 30 días naturales serían necesarios para completar todo el proceso (unas 4 semanas).

Fase	Descripción de la fase	Duración
Fase 1: documentación SOC	Analistas deben leer y asimilar documentación del SIEM	5 días laborables
Fase 2: documentación SIEM	Analistas deben entender el funcionamiento del SIEM en exclusiva	5 días laborables
Fase 3: seguimiento a analistas senior	Analistas deben seguir y trabajar observando a los analistas senior.	5 días laborables
Fase 4: Analistas trabajan en entorno de test	Analistas trabajan supervisados en un entorno de pruebas	5 días laborables

Fase 1: Introducción a la documentación del SOC

En esta fase, los analistas se familiarizan con los procesos y documentaciones internas del SOC, normalmente, en este periodo también deberían adaptarse a los procesos internos de la propia Fincomp. Es una fase de teoría pura. El analista en este paso tendría una visión más general del SOC, teniendo contacto con otras partes de este, como ingeniería, inteligencia y otras.

Fase 2: Introducción a la documentación SIEM

En esta fase el analista se centrará específicamente en cómo el SIEM y sus herramientas complementarias funcionan, con videotutoriales, cursos, y manuales complementarios. El acceso a las certificaciones de los vendedores SIEM podría estar contemplada por la empresa en este punto.

Fase 3: Seguimiento a analistas senior o ¨Shadowing¨

Llegados a este punto, cada nuevo analista sería asignado a un analista senior. A la vez que el analista senior realiza sus tareas diarias, ejercería como profesor del nuevo analista, enseñando cómo se realiza un análisis correctamente, además de mostrar las herramientas de uso diario, procesos requeridos y otros aspectos que podrían no estar documentados y basarse en las experiencias (atajos en búsquedas, uso de lenguaje de búsqueda en lugar del asistente, páginas de análisis interesantes…). En esta fase se podría comenzar a evaluar el trabajo del nuevo analista por parte del senior, cediendo el control en algún aspecto de las tareas diarias.

Fase 4: Inicio de la monitorización en entorno de pruebas

En la fase final del entrenamiento, el analista comenzaría a trabajar por su cuenta, analizando ofensas y respondiendo a éstas en un entorno de pruebas. Estas ofensas serían analizadas a diario por un analista senior, y enviadas en un reporte al manager, para llevar un seguimiento de la aptitud y el rigor en el análisis. En esta fase también se podrían comenzar a delegar parte de las tareas diarias en producción, las cuales no requieren grandes responsabilidades, para familiarizarse con ellas.

A partir de este punto, el manager y los analistas senior decidirán la viabilidad del nuevo analista. Comenzando a monitorizar alertas en producción y realizando las tareas diarias asignadas.

Referencias

SOC-SOP-0006-Monitorización de alertas

SOC-SOP-0007-Escalación de posibles incidentes de seguridad

Reunión Semanal - Semana 1 - 9 de marzo de 2020

Estado del documento	COMPLETADO
Fecha creación	09 Mar 2020
Creador	@ Daniel Rodríguez Fueyo
Responsable	@ Daniel Rodríguez Fueyo
Ultima fecha de revisión	10 Mar 2020

- Descripción de la reunión
- Fecha
- Participantes
- Objetivos
- Temas discutidos
- Medidas propuestas
- Decisiones tomadas
- Cambios en el documento

Descripción de la reunión

Reunión semanal para decisiones de implementación y gestión del nuevo SOC.

Fecha

09 Mar 2020

Participantes

Lista de participantes e invitados necesarios en la reunión:

Puesto	Participación	Estado final
@ Daniel Rodríguez Fueyo - Manager del SOC	OBLIGATORIA	PARTICIPANTE -PRESENCIAL
Service Delivery Manager	OBLIGATORIA	PARTICIPANTE -PRESENCIAL
SOC team leader	OPCIONAL	PARTICIPANTE - REMOTO
Ingeniero del SOC	OPCIONAL	PARTICIPANTE -PRESENCIAL

Objetivos

- Presentación del equipo.
- Seguimiento general del proyecto.
- Instrucciones para comenzar la instalación del hardware en la zona de test.

Temas discutidos

Elemento	Iniciador	Notas
Presentación del equipo y objetivo de las reuniones	@ Daniel Rodríguez Fuey	• Breve introducción del equipo y de los objetivos a alcanzar en este tipo de reuniones.
Verificación de los presupuestos para los SIEM	@ Daniel Rodríguez Fuey	• Presentación por parte del manager de la elección de los SIEM a implementar.

Muestra de la plantilla a utilizar para documentar las reuniones	@ Daniel Rodríguez Fuey	• Revisión del modelo a utilizar, sugerencias y cambios a éste y aprobación.

Medidas propuestas

- [x] Aprobación presupuestos
- [x] Propuesta para aprobar la plantilla a utilizar

Decisiones tomadas

Se comenzará con la implementación de los SIEM elegidos

Se utilizará el modelo de plantilla aprobado a partir de ahora para todo el proyecto.

Cambios en el documento

Fecha del cambio	Editor	Descripción del cambio
09 Mar 2020	@ Daniel Rodríguez Fueyo	Creación del documento antes de la reunión
10 Mar 2020	@ Daniel Rodríguez Fueyo	Documento completado con los apuntes de la reunión celebrada

Reunión Semanal - Semana 2 - 16 de marzo de 2020

Estado del documento	COMPLETADO
Fecha creación	16 Mar 2020
Creador	@ Daniel Rodríguez Fueyo
Responsable	Ingeniero del SOC @ Daniel Rodríguez Fueyo
Ultima fecha de revisión	17 Mar 2020

- Descripción de la reunión
- Fecha
- Participantes
- Objetivos
- Temas discutidos
- Medidas propuestas
- Decisiones tomadas
- Cambios en el documento

Descripción de la reunión

Reunión semanal para decisiones de implementación y gestión del nuevo SOC.

Fecha

16 Mar 2020

Participantes

Lista de participantes e invitados necesarios en la reunión:

Puesto	Participación	Estado final
@ Daniel Rodríguez Fueyo - Manager del SOC	OBLIGATORIA	PARTICIPANTE -PRESENCIAL
Service Delivery Manager	OBLIGATORIA	PARTICIPANTE -PRESENCIAL
SOC team leader	OBLIGATORIA	PARTICIPANTE - REMOTO
Ingeniero del SOC	OBLIGATORIA	PARTICIPANTE -PRESENCIAL

Objetivos

- Discutir el avance de la implementación del hardware en la infraestructura.
- Revisión del avance del proyecto.
- Toma de decisiones acerca de procedimientos.

Temas discutidos

Elemento	Presenter	Notas
Estado de los elementos insertados en zona pre- producción	Ingeniero SOC	• Información acerca de los conectores insertados en TEST, parecen funcionar. Se continuará con la inclusión de los log Sources y pruebas de conectividad. • Petición de inclusión de conectores en zona DMZ.
Petición de creación de Runbooks para documentación en Confluence.	Ingeniero SOC	• Verificación con dirección para la aplicación o no de los procesos de instalación de los SIEM.
Presentación del estado del proyecto por parte de dirección	@ Daniel Rodríguez Fuey	• Introducción de decisiones tomadas hasta este punto y los puntos a comenzar: 1. Propuesta de creación de procedimientos requeridos por auditoria Fincomp.

Medidas propuestas

- [x] Continuación con la instalación del hardware y conectividad. Extensión a zona DMZ
- [x] Creación de runbooks para instalaciones

Decisiones tomadas

Denegado: Los runbooks serán proporcionados por los fabricantes del SIEM, información considerada redundante. No se continuarán con ellos a menos que se vea necesario.

Aceptado: Extensión de la inclusión de conectores en zona DMZ (basada en Linux principalmente -rsyslog).

Aceptado: Comenzar a verificar con departamento de redes el envío de eventos desde los dispositivos de test.

Cambios en el documento

Fecha del cambio	Editor	Descripción del cambio
16 Mar 2020	@ Daniel Rodríguez Fueyo	Creación del documento antes de la reunión
17 Mar 2020	@ Daniel Rodríguez Fueyo	Documento completado con los apuntes de la reunión celebrada

Reunión Semanal - Semana 3 - 23 de marzo de 2020

Estado del documento	COMPLETADO
Fecha creación	23 Mar 2020
Creador	@ Daniel Rodríguez Fueyo
Responsable	SOC Team Leader, Ingeniero SOC, @ Daniel Rodríguez Fueyo
Ultima fecha de revisión	23 Mar 2020

Descripción de la reunión

Reunión semanal para decisiones de implementación y gestión del nuevo SOC.

Fecha

23 Mar 2020

Participantes

Lista de participantes e invitados necesarios en la reunión:

Puesto	Participación	Estado final
@ Daniel Rodríguez Fueyo - Manager del SOC	OBLIGATORIA - RESPONSABLE	PARTICIPANTE -PRESENCIAL
Service Delivery Manager	OBLIGATORIA	PARTICIPANTE -PRESENCIAL
SOC team leader	OBLIGAORIA - PRESENTA	PARTICIPANTE - REMOTO
Ingeniero del SOC	OBLIGATORIA - PRESENTA	PARTICIPANTE -PRESENCIAL

Objetivos

- Verificar el estado de cada parte del proyecto para la semana indicada.
- Toma de decisiones para los siguientes pasos a realizar.

Temas discutidos

Elemento	Presenter	Notas
Estado de la implementación de hardware	Ingeniero SOC	• Confirmación de que los colectores han sido colocados en DMZ. Prueba de conectividad a la consola con éxito. • Conectividad limitada para los logs de Test. En algunos sistemas Windows Wincollect no está instalado, es necesario más tiempo. Se • debe priorizar terminar esta tarea al extender el hardware.
Creación de procedimientos para analistas	SOC team leader	• Procedimientos iniciados por la sección de analistas. No hay consenso en cómo proceder con el referente a la creación de estadísticas.

Descripción del estado del proyecto	@ Daniel Rodríguez Fuey	información acerca de las fechas límite para la entrega de procedimientos deben estar terminados al final de la fase 2 (17 May 2020). Nuevos analistas confirmados para empezar a mediados del mes de Mayo. Procedimiento de entrenamiento de analistas debe estar listo.

Medidas propuestas

- [x] Paro temporal de la introducción de hardware para solucionar problemas con los colectores Windows.
- [x] Pregunta acerca del proceder con el procedimiento de estadísticas y reportes (no está claro)

Decisiones tomadas

Aceptado: Se revisará el poder implementar los colectores antes de proceder más adelante.

Denegado: El procedimiento de Reportes queda cancelado. El formato dependerá del equipo que requiera los datos y lo que se proporcione.

Cambios en el documento

Fecha del cambio	Editor	Descripción del cambio
23 Mar 2020	@ Daniel Rodríguez Fueyo	Creación del documento con los aspectos de la reunión.

Reunión Semanal - Semana 4 - 30 de marzo de 2020

Estado del documento	COMPLETADO
Fecha creación	30 Mar 2020
Creador	@ Daniel Rodríguez Fueyo
Responsable	N/A
Ultima fecha de revisión	30 Mar 2020

Descripción de la reunión

Reunión semanal para decisiones de implementación y gestión del nuevo SOC.

Fecha

30 Mar 2020

Participantes

Lista de participantes e invitados necesarios en la reunión:

Puesto	Participación	Estado final

@ Daniel Rodríguez Fueyo - Manager del SOC	OBLIGATORIA	PARTICIPANTE -PRESENCIAL
Service Delivery Manager	OBLIGATORIA -PRESENTA	PARTICIPANTE - REMOTO
SOC team leader	OBLIGATORIA - PRESENTA	PARTICIPANTE - PRESENCIAL
Ingeniero del SOC	OBLIGARTORIA - PRESENTA	PARTICIPANTE -PRESENCIAL

Objetivos

- Decisiones acerca de los siguientes pasos en el proyecto.

Temas discutidos

Elemento	Presenter	Notas
Comienzo de trabajo en los Casos de Uso	Service delivery Manager	• Comienzo del trabajo en el procedimiento usado para crear los casos de uso
Estado de la implementación del hardware	Ingeniero SOC	• Logs funcionan en DMZ y Test • Se comienza a implementar en Zona Usuario • Reuniones para gestionar implementación en SSLVPN y Proxies
Información general del proyecto	@ Daniel Rodríguez Fuey	• Pedida de recolección de incidencias para reunión mensual con el CISO. • Verificación del estado del proyecto: ligero retraso en hardware.
Información acerca de los procedimientos de analista y monitorización	SOC Team leader	• Petición de información a ingeniería para trabajar en los procedimientos de modificación y prueba de reglas.

Medidas propuestas

- [x] Envío de información a dirección para añadir a la presentación mensual.
- [x] Continuar con la implementación en Zona usuario y paralelamente en SSLVPN para optimizar tiempo.

Decisiones tomadas

Aceptado: Se trabajará paralelamente en ambas zonas, ya que más tarde el hardware se ralentizará debido a la asignación de recursos en la configuración de los SIEM.

Aceptado: Asignación de 3 horas de ingeniería para trabajar en los procedimientos necesarios.

Cambios en el documento

Fecha del cambio	Editor	Descripción del cambio
30 Mar 2020	@ Daniel Rodríguez Fueyo	Documento completado con los apuntes de la reunión celebrada.

Reunión Semanal - Semana 5 - 6 de abril de 2020

Estado del documento	COMPLETADO
Fecha creación	06 Apr 2020
Creador	@ Daniel Rodríguez Fueyo
Responsable	N/A

Ultima fecha de revisión	06 Apr 2020

- Descripción de la reunión
- Fecha
- Participantes
- Objetivos
- Temas discutidos
- Medidas propuestas
- Decisiones tomadas
- Cambios en el documento

Descripción de la reunión

Reunión semanal para decisiones de implementación y gestión del nuevo SOC.

Fecha

06 Apr 2020

Participantes

Lista de participantes e invitados necesarios en la reunión:

Puesto	Participación	Estado final
@ Daniel Rodríguez Fueyo - Manager del SOC	OBLIGATORIA - PRESENTA	PARTICIPANTE -PRESENCIAL
Service Delivery Manager	OBLIGATORIA	PARTICIPANTE -PRESENCIAL
SOC team leader	OBLIGATORIA -PRESENTA	PARTICIPANTE -PRESENCIAL
Ingeniero del SOC	OBLIGATORIA - PRESENTA	PARTICIPANTE -PRESENCIAL

Objetivos

- Verificación del estado del proyecto y toma de decisiones acerca de los siguientes pasos a realizar

Temas discutidos

Elemento	Presenter	Notas
Implementación de hardware	Ingeniero del SOC	• Conectores de zona usuario y SSLVPN agregados. Se continua con la inclusión de los log sources de la VPN y una parte de los de zona Usuario (endpoints -Windows). Zona delegaciones en progreso. Se espera comenzar con producción en unas dos semanas.
Implementación del Software	Ingeniero del SOC	• Se comienza con la instalación de las consolas en la zona SOC (la zona SOC contiene el conector local, no hace falta agregar uno nuevo). Plazo estimado de un mes.
Finalización del proceso para casos de uso	Service Delivery Manager	• Se presenta el procedimiento a utilizar cuando se requiere implementar un nuevo caso de uso, requiere aprobación de dirección.
Comienzo de implementación de casos de uso	Service Delivery Manager	• Primeras reuniones con otros departamentos para implementar los primeros casos de uso.

Medidas propuestas

- [x] Confirmación de los pasos de la instalación de hardware y la introducción de la configuración de software.
- [x] Aprobación del procedimiento SOC-SOP-0001-Implementación de Casos de Uso (CU)

Decisiones tomadas

Aprobado procedimiento SOC-SOP-0001-Implementación de Casos de Uso (CU)

Aprobado el proceder con la instalación de software.

Cambios en el documento

Fecha del cambio	Editor	Descripción del cambio
06 Apr 2020	@ Daniel Rodríguez Fueyo	Documento completado con los apuntes de la reunión celebrada.

Reunión Semanal - Semana 6 - 13 de abril de 2020

Estado del documento	COMPLETADO
Fecha creación	13 Apr 2020
Creador	@ Daniel Rodríguez Fueyo
Responsable	N/A
Ultima fecha de revisión	13 Apr 2020

- Descripción de la reunión
- Fecha
- Participantes
- Objetivos
- Temas discutidos
- Medidas propuestas
- Decisiones tomadas
- Cambios en el documento

Descripción de la reunión

Reunión semanal para decisiones de implementación y gestión del nuevo SOC.

Fecha

13 Apr 2020

Participantes

Lista de participantes e invitados necesarios en la reunión:

Puesto	Participación	Estado final
@ Daniel Rodríguez Fueyo - Manager del SOC	OBLIGATORIA - PRESENTA	PARTICIPANTE -PRESENCIAL
Service Delivery Manager	OBLIGATORIA	AUSENTE
SOC team leader	OBLIGATORIA - PRESENTA	PARTICIPANTE - REMOTO
Ingeniero del SOC	OBLIGATORIA -PRESENTA	PARTICIPANTE -PRESENCIAL

Objetivos

- Verificación del estado del proyecto.

Temas discutidos

Elemento	Presenter	Notas
Presentación de procedimientos terminados para aprobación	SOC team lead	• Muestra de los procedimientos para su verificación por parte de la dirección 1. Cómo crear playbooks 2. Testeo de reglas e implementación
Información del estado de la implementación del hardware y software	Ingeniero del SOC	• Problemas para la implementación de los conectores en las sedes, los envíos de material se retrasan para ser implementados. • Resto de los conectores, a excepción de producción insertados. Pruebas de envíos de eventos en progreso. Aprobación para comenzar a incluir producción. • Consolas instaladas, se podrá proceder a la inclusión de aplicaciones y correlación de eventos. Se comienza a configurar los procesadores adicionales.
Descripción del estado del proyecto y pequeñas actualizaciones de la parte del cliente.	@ Daniel Rodríguez Fuey	• Se reforzará con un ingeniero más las tareas de implementación (consultor) durante un mes, para ayudar en las tareas de hardware. • Comenzarán la implementación de reglas y casos de uso, se necesitará desviar horas de trabajo de los ingenieros para estas tareas.

Medidas propuestas

- [x] Incluir producción en el hardware de los SIEM.
- [x] Aprobación de los procedimientos SOC-SOP-0004-Creación y mantenimiento de Libros de reglas (Playbooks) y SOC-SOP-0002-Implementación y prueba de reglas en SIEM

Decisiones tomadas

Denegado: no se incluye producción de momento, se ha preferido terminar el resto de zonas para tener luz verde para producción (se necesita tiempo durante el fin de semana para esta tarea).

procedimientos SOC-SOP-0004-Creación y mantenimiento de Libros de reglas (Playbooks) y SOC-SOP-0002-Implementación y prueba de reglas en SIEM quedan aprobados.

Se incorporará un consultor (ingeniero) durante 30 días.

Cambios en el documento

Fecha del cambio	Editor	Descripción del cambio
13 Apr 2020	@ Daniel Rodríguez Fueyo	Documento completado con los apuntes de la reunión celebrada.

Reunión Semanal - Semana 7 - 20 de abril de 2020

Estado del documento	COMPLETADO
Fecha creación	20 Apr 2020
Creador	@ Daniel Rodríguez Fueyo
Responsable	N/A
Ultima fecha de revisión	20 Apr 2020

- Descripción de la reunión
- Fecha

- Participantes
- Objetivos
- Temas discutidos
- Medidas propuestas
- Decisiones tomadas
- Cambios en el documento

Descripción de la reunión

Reunión semanal para decisiones de implementación y gestión del nuevo SOC.

Fecha

20 Apr 2020

Participantes

Lista de participantes e invitados necesarios en la reunión:

Puesto	Participación	Estado final
@ Daniel Rodríguez Fueyo - Manager del SOC	OBLIGATORIA -PRESENTA	PARTICIPANTE -PRESENCIAL
Service Delivery Manager	OBLIGATORIA -PRESENTA	PARTICIPANTE -PRESENCIAL
SOC team leader	OBLIGATORIA	PARTICIPANTE - PRESENCIAL
Ingeniero del SOC	OBLIGATORIA -PRESENTA	PARTICIPANTE -PRESENCIAL

Objetivos

- Verificación del estado del proyecto

Temas discutidos

Elemento	Presenter	Notas
Actualización de los puntos de implementación del hardware y Software.	Ingeniero del SOC	• Finalización de la inclusión de los conectores en las sedes, la conectividad se ha verificado. • Se procede a incluir los eventos de los dispositivos restantes en las demás zonas (impresoras, proxy, antivirus…) • Prueba de testeo de reglas por defecto funciona en todas las zonas menos en DMZ, hay un problema en la conectividad con los servidores Linux, los Firewalls bloquean los envíos. • Petición de un slot para incluir el hardware en producción. • Retraso en la parte software al centrarse en casos de uso y en hardware. Se reanudará después de incluir el hardware en producción.
Información general	@ Daniel Rodríguez Fueyo	• Presentación del nuevo Consultor • Información del estado del proyecto.
Verificación de los primeros casos de uso.	Service Delivery Manager	Actualización del estado de algunos casos de Uso, problemas entre la expectativa e información de los departamentos y las posibilidades de implementación reales.

Medidas propuestas

- [x] Incluir un hueco en las ventanas de actualización para incluir el nuevo hardware en producción.

Decisiones tomadas

Acuerdo: @ Daniel Rodríguez Fueyo inicia el procedimiento de petición de la implementación en producción.

Cambios en el documento

Fecha del cambio	Editor	Descripción del cambio
20 Apr 2020	@ Daniel Rodríguez Fueyo	Documento completado con los apuntes de la reunión celebrada.

Reunión Semanal - Semana 8 - 27 de abril de 2020

Estado del documento	COMPLETADO
Fecha creación	27 Apr 2020
Creador	@ Daniel Rodríguez Fueyo
Responsable	N/A
Ultima fecha de revisión	27 Apr 2020

- Descripción de la reunión
- Fecha
- Participantes
- Objetivos
- Temas discutidos
- Medidas propuestas
- Decisiones tomadas
- Cambios en el documento

Descripción de la reunión

Reunión semanal para decisiones de implementación y gestión del nuevo SOC.

Fecha

27 Apr 2020

Participantes

Lista de participantes e invitados necesarios en la reunión:

Puesto	Participación	Estado final
@ Daniel Rodríguez Fueyo - Manager del SOC	OBLIGATORIA	PARTICIPANTE -PRESENCIAL
Service Delivery Manager	OBLIGATORIA	PARTICIPANTE -PRESENCIAL
SOC team leader	OBLIGATORIA - PRESENTA	PARTICIPANTE - REMOTO
Ingeniero del SOC	OBLIGATORIA	PARTICIPANTE -PRESENCIAL

Objetivos

- Verificación del estado del proyecto.

Temas discutidos

Elemento	Presenter	Notas
Información acerca de implementación de hardware y software	Ingeniero SOC	• Ventana para implementación de hardware en producción 02 May 2020 • Resto de redes envían los eventos. • Software: Se comenzará a configurar los accesos para el equipo. Se procede a modificar y adaptar el formato de los eventos para que muestre la información de forma correcta (antes los eventos eran genéricos, solamente se comprobó que llegaban) • Creación de las primeras reglas a partir de los casos de uso.
Otras cuestiones	@ Daniel Rodríguez Fuey	• Petición de información para presentación de final de mes con el CISO.
Avances procedimientos	SOC team lead	• Información acerca de los procedimientos en progreso. • Se comienza a discutir como implementar los libros de reglas.

Medidas propuestas

- [x] Muestra de información, no hay puntos a proponer

Decisiones tomadas

Continuación de las operaciones según lo previsto

Cambios en el documento

Fecha del cambio	Editor	Descripción del cambio
27 Apr 2020	@ Daniel Rodríguez Fueyo	Documento completado con los apuntes de la reunión celebrada.

Reunión Semanal - Semana 9 - 4 de mayo de 2020

Estado del documento	COMPLETADO
Fecha creación	04 May 2020
Creador	@ Daniel Rodríguez Fueyo
Responsable	N/A
Ultima fecha de revisión	04 May 2020

Descripción de la reunión

Reunión semanal para decisiones de implementación y gestión del nuevo SOC.

Fecha

04 May 2020

Participantes

Lista de participantes e invitados necesarios en la reunión:

Puesto	Participación	Estado final
@ Daniel Rodríguez Fueyo - Manager del SOC	OBLIGATORIA	AUSENTE
Service Delivery Manager	OBLIGATORIA	PARTICIPANTE -PRESENCIAL
SOC team leader	OBLIGATORIA - PRESENTA	PARTICIPANTE - PRESENCIAL
Ingeniero del SOC	OBLIGATORIA -PRESENTA	PARTICIPANTE -PRESENCIAL

Objetivos

- Verificación y aprobación de cambios en el proyecto.

Temas discutidos

Elemento	Presenter	Notas
Instalación de software terminada.	Ingeniero SOC	• Acceso granular para los miembros del SOC terminado, cuentas creadas en todos los dispositivos para los analistas, ingenieros, manager y SDM.
Instalación de hardware en producción.	Ingeniero SOC	• instalación ejecutada en la ventana aprobada en el 02 May 2020. Problemas con la inclusión de uno de los colectores, pero solucionada después de unas horas. Logs de muestra recibidos, de máquinas en Mainframe, Tandem, LDAP y servidores Windows, Linux. • La instalación de hardware puede darse por finalizada a falta de verificación de pequeños eventos.
Verificación y aprobación de procedimientos	SOC team leader	• Muestra de los procedimientos terminados para aprobación 1. Escalación de incidente. 2. modificación y mejora de reglas SIEM.

Medidas propuestas

- [x] Aprobación de procedimientos SOC-SOP-0007-Escalación de posibles incidentes de seguridad y SOC-SOP-0008-Modificación y mejora de reglas SIEM
- [x] Verificación de cierre de la fase de implementación de hardware, para asignación de recursos a software, reglas y casos de uso.

Decisiones tomadas

Aprobados procedimientos por parte del SDM @ Daniel Rodriguez fueyo se encuentra ausente.

Aprobada desviación de recursos. Un ingeniero se mantiene para verificar posibles problemas de hardware.

Cambios en el documento

Fecha del cambio	Editor	Descripción del cambio
04 May 2020	@ Daniel Rodríguez Fueyo	Documento completado con los apuntes de la reunión celebrada.

Reunión Semanal - Semana 10 - 11 de mayo de 2020

Estado del documento	COMPLETADO
Fecha creación	11 May 2020
Creador	@ Daniel Rodríguez Fueyo
Responsable	N/A
Ultima fecha de revisión	11 May 2020

- Descripción de la reunión
- Fecha
- Participantes
- Objetivos
- Temas discutidos
- Medidas propuestas
- Decisiones tomadas
- Cambios en el documento

Descripción de la reunión

Reunión semanal para decisiones de implementación y gestión del nuevo SOC.

Fecha

11 May 2020

Participantes

Lista de participantes e invitados necesarios en la reunión:

Puesto	Participación	Estado final
@ Daniel Rodríguez Fueyo - Manager del SOC	OBLIGATORIA	PARTICIPANTE -PRESENCIAL
Service Delivery Manager	OBLIGATORIA	PARTICIPANTE -PRESENCIAL
SOC team leader	OPCIONAL	PARTICIPANTE - REMOTO
Ingeniero del SOC	OPCIONAL	PARTICIPANTE -PRESENCIAL

Objetivos

- Aprobación y verificación del estado de algunas acciones pasadas y futuras del proyecto.

Temas discutidos

Elemento	Presenter	Notas
Actualización semanal	@ Daniel Rodríguez Fuey	• Información general tras reunión con el CISO y pequeñas actualizaciones. Analistas comienzan durante esta semana y la siguiente. • Verificación con Ingeniería de que el consultor contratado sigue siendo necesario al terminar la parte de hardware. •
Muestra y aprobación	SOC Team leader	• Muestra para aprobación de un nuevo procedimiento terminado. • 1. Entrenamiento para analistas.

Fase de implementación de software y alertas.	Ingeniero SOC	Reglas implementadas en los siem a partir de los casos de uso, en fase de pruebas (no generan alertas) Petición para activar alertas en los SIEM como prueba.
Verificación de casos de uso con departamentos externos	Service Delivery Manager	Muestra del planning de actuación para futuros casos de uso (priorización) y calendario de objetivos para estos. Muchos se encuentran fuera del proyecto y son para la fase permanente.

Medidas propuestas

- [x] aprobación de procedimiento SOC-SOP-0003-Entrenamiento para analistas
- [x] Activación de ofensas con las reglas creadas.
- [x] Propuesta para mantener al consultor durante el tiempo inicial (1 mes) para labores de soporte en reglas y configuración

Decisiones tomadas

Aprobado procedimiento: SOC-SOP-0003-Entrenamiento para analistas

Denegado: Las reglas deben ser activadas si existe un libro de reglas acorde, si no se dispone de él se debe actuar en un entorno de pruebas, no con las redes de la empresa.

Aprobado: Consultor continúa hasta el viernes 22 May 2020 para labores de soporte.

Cambios en el documento

Fecha del cambio	Editor	Descripción del cambio
11 May 2020	@ Daniel Rodríguez Fueyo	Documento completado con los apuntes de la reunión celebrada.

Reunión Semanal - Semana 11 - 18 de mayo de 2020

Estado del documento	COMPLETADO
Fecha creación	18 May 2020
Creador	@ Daniel Rodríguez Fueyo
Responsable	N/A
Ultima fecha de revisión	18 May 2020

Descripción de la reunión

Reunión semanal para decisiones de implementación y gestión del nuevo SOC.

Fecha

18 May 2020

Participantes

Lista de participantes e invitados necesarios en la reunión:

Puesto	Participación	Estado final
@ Daniel Rodríguez Fueyo - Manager del SOC	OBLIGATORIA - PRESENTA	PARTICIPANTE -PRESENCIAL
Service Delivery Manager	OBLIGATORIA - PRESENTA	PARTICIPANTE -PRESENCIAL
SOC team leader	OBLIGATORIA - PRESENTA	PARTICIPANTE - PRESENCIAL
Ingeniero del SOC	OBLIGATORIA - PRESENTA	PARTICIPANTE -PRESENCIAL

Objetivos

- Verificación del estado del proyecto antes de comenzar con las priorizaciones (Fase 3).

Temas discutidos

Elemento	Presenter	Notas
Nuevos analistas comienzan en la empresa	@ Daniel Rodríguez Fuey	• Comienzo del entrenamiento de los nuevos analistas. Familiarización con los procesos internos de la empresa y documentación. • Debe enviarse un reporte semanal de la actividad de cada uno para verificar si los analistas adquieren el conocimiento necesario antes de entrar a monitorizar alertas reales.
Aprobación de procedimientos pendientes y finalización de estos.	SOC team lead, Service Delivery Manager.	Dos últimos procedimientos son mostrados para verificación y aprobación. 1. Monitorización de alertas. 2. Recuperación ante desastres. Confirmación de cierre de los procedimientos. Si alguno adicional fuera necesario se realizaría bajo petición expresa de dirección.
Operaciones: Libros de reglas, reglas y casos de uso	Ingeniero SOC	• comienzan a generarse los libros de reglas para los analistas. • Más reglas empiezan a probarse y finalizarse. • Trabajo en casos de uso con SDM, se requiere aprobar un objetivo semanal. Propuesta de dos casos de uso como máximo por semana.
Implementación: pequeños problemas con los formatos de los logs recibidos	Ingeniero SOC	Sistemas antiguos como Mainframe y Tandem no disponen de sistemas para organizar los eventos de forma automática, el parsing de eventos debe realizarse de forma manual, campo a campo. Pequeños problemas con algunos sistemas en el envío de logs están siendo solucionados por equipos externos. Tickets de seguimiento han sido enviados.

Medidas propuestas

- [x] Creación de reporte sobre el estado de los analistas.
- [x] Aprobación de procedimientos SOC-SOP-0006-Monitorización de alertas y SOC-SOP-0005-Plan de recuperación ante desastres (Disaster Recovery)
- [x] Aprobación de objetivo de casos de uso semanales.

Decisiones tomadas

Aprobado: creación de reporte semanal por parte del SOC team leader para realizar seguimiento.

Aprobados los libros de reglas y se da por finalizado este segmento.

Se aprueba el objetivo: no se podrá requerir más de dos casos para no sobrecargar a los ingenieros de trabajo.

Cambios en el documento

Fecha del cambio	Editor	Descripción del cambio
18 May 2020	@ Daniel Rodríguez Fueyo	Documento completado con los apuntes de la reunión celebrada.

Reunión Semanal - Semana 12 - 25 de mayo de 2020

Estado del documento	COMPLETADO
Fecha creación	25 May 2020
Creador	@ Daniel Rodríguez Fueyo
Responsable	N/A
Ultima fecha de revisión	25 May 2020

- Descripción de la reunión
- Fecha
- Participantes
- Objetivos
- Temas discutidos
- Medidas propuestas
- Decisiones tomadas
- Cambios en el documento

Descripción de la reunión

Reunión semanal para decisiones de implementación y gestión del nuevo SOC.

Fecha

25 May 2020

Participantes

Lista de participantes e invitados necesarios en la reunión:

Puesto	Participación	Estado final
@ Daniel Rodríguez Fueyo - Manager del SOC	OBLIGATORIA - PRESENTA	PARTICIPANTE -PRESENCIAL
Service Delivery Manager	OBLIGATORIA - PRESENTA	PARTICIPANTE -PRESENCIAL
SOC team leader	OBLIGATORIA - PRESENTA	PARTICIPANTE - PRESENCIAL
Ingeniero del SOC	OBLIGATORIA - PRESENTA	PARTICIPANTE -PRESENCIAL

Objetivos

- Verificación de las distintas secciones del proyecto se van completando.
- Priorización de tareas para llegar en tiempo a la fecha final de entrega: 08 Jun 2020

Temas discutidos

Elemento	Presenter	Notas
Cierre de secciones y estado de cada una	@ Daniel Rodríguez Fueyo	• Se requiere verificación del estado de cada fase, para observar si se ha completado. • En caso de no haberse hecho, se verificará si se pueden desviar recursos para agilizar su finalización.
Estado de fases de implementación	Ingeniero SOC	• Implementación hardware completada: Si existe algún incidente se resolverá mediante un ticket de intervención. No se requieren recursos adicionales. • Implementación de software: Excepto algunos errores de las versiones de software, todos los elementos se encuentran activos y listos para trabajo. Se puede considerar cerrada.
Estado de operaciones: Ingeniería	Ingeniero SOC	• Casos de uso: En progreso. Se continuará al finalizar el proyecto, es un objetivo para el estado permanente. Ingenieros que trabajan en el software han sido incluidos a partir de ahora en esta tarea. • Reglas: Reglas básicas funcionan. Se comienzan a implementar reglas basadas en los casos de uso que se reciben. El ingeniero que trabajaba en la sección de hardware ha sido desviado a esta tarea. Libros de reglas: Un ingeniero actúa de soporte a los analistas senior para ayudar a la aprobación y creación de estos. Requerimiento de aprobación para activación de reglas con los libros aprobados.
Estado de entrenamiento de nuevos analistas	SOC team lead	Reporte enviado a @ Daniel Rodríguez Fueyo sobre los analistas. • Analistas Senior preparados para monitorización de reglas. De acuerdo en activar monitorización para las reglas por defecto. • Comienza la introducción a los SIEM para los nuevos analistas.
Recopilación de información para informe a los auditores	Service Delivery Manager	• Los auditores requieren un primer informe de los casos de uso, reglas y libros creados. También se pide un informe de 5 alertas al azar para observar la respuesta del SOC ante ellas. • Fecha de entrega: cierre de proyecto 08 Jun 2020

Medidas propuestas

- [x] Requerido informe de cada sección para la semana que viene sobre el estado de cada punto.
- [x] Petición de cierre de implementación de hardware y software.
- [x] Asignación de los ingenieros de implementación para operaciones.
- [x] Petición de activación de reglas para monitorización (efecto inmediato).

Decisiones tomadas

Aprobado: Cierre de Implementaciones.

Aprobado: Se asignan a los ingenieros a operaciones. Actuación en implementación basándose en prioridad de incidente.

Aprobado: Reglas con su libro aprobado pueden activarse en la red de la empresa.

Requerido: Información detallada para proceder al comienzo del cierre de proyecto. Inclusión de gastos y tiempo empleado para cada acción.

Cambios en el documento

Fecha del cambio	Editor	Descripción del cambio
25 May 2020	@ Daniel Rodríguez Fueyo	Documento completado con los apuntes de la reunión celebrada.

Reunión Semanal - Semana 13 - 1 de junio de 2020

Estado del documento	COMPLETADO
Fecha creación	01 Jun 2020
Creador	@ Daniel Rodríguez Fueyo
Responsable	N/A
Ultima fecha de revisión	01 Jun 2020

- Descripción de la reunión
- Participantes
- Objetivos
- Temas discutidos
- Medidas propuestas
- Decisiones tomadas
- Cambios en el documento

Descripción de la reunión

Reunión semanal para decisiones de implementación y gestión del nuevo SOC.

Participantes

Lista de participantes e invitados necesarios en la reunión:

Puesto	Participación	Estado final
@ Daniel Rodríguez Fueyo	OBLIGATORIA - PRESENTA	PARTICIPANTE -PRESENCIAL
Service Delivery Manager	OBLIGATORIA - PRESENTA	PARTICIPANTE -PRESENCIAL
SOC team leader	OBLIGATORIA - PRESENTA	PARTICIPANTE - PRESENCIAL
Ingeniero del SOC	OBLIGATORIA - PRESENTA	PARTICIPANTE -PRESENCIAL

Objetivos

- Obtención de la información para proceder con el cierre del proyecto la última semana.
- Revisión de documentos para entrega.

Temas discutidos

Elemento	Presenter	Notas
Cierre de proyectos - lecciones aprendidas	@ Daniel Rodríguez Fuey	• información del proyecto antes de comenzar con el cierre. • Obtención de información para observar puntos fallidos y cómo se podían haber solucionado. • Finalización de las reuniones semanales debido al final del proyecto de implementación.

Estado de los proyectos de ingeniería	Ingeniero SOC	• Implementaciones: finalizadas • Operaciones: 1. Casos de uso: proceso implementado y listo para el final del proyecto 2. Reglas: Reglas básicas implementadas, listo para continuar al finalizar el proyecto. 3. Libros de reglas: procedimientos implementados y libros requeridos creados, listo para continuar el proyecto. Sección de ingeniería lista para el cierre de proyecto. Las tareas pendientes se desarrollarán en un largo plazo. Nuevas alertas tendrán que ser generadas de forma continua.
Estado de la monitorización del SOC	SOC Team lead	• Nuevos analistas comienzan a verificar alertas con los analistas senior. • Muestras de análisis de alertas creadas. • A partir de la próxima semana los analistas podrán trabajar de forma autónoma bajo supervisión de los seniors. • Monitorización preparada para el cierre de proyecto. Para el futuro más analistas deberán incluirse dependiendo del número de reglas implementadas (las alertas podrían aumentar mucho)
Estado de la gestión y requerimientos	Service Delivery Manager	• Verificación de documentos para entrega. Algunos puntos a mejorar en los procedimientos para entrega (pequeñas modificaciones). • Petición de análisis para 5 alertas (auditores): 1. SOC-RC-0001-Intentos múltiples de autenticación fallidos 2. SOC-RC-0002-Comandos sospechosos ejecutados 3. SOC-RC-0003-Actividad relacionada con un posible Cryptolocker 4. SOC-RC-0004-Posible escáner de red detectado (Local-Local) 5. SOC-RC-0005-Conexión a una página potencialmente peligrosa (En lista negra-Blacklist)

Medidas propuestas

- [x] Cierre de proyecto.
- [x] Verificación de que las actividades deben ser realizables en el proyecto permanente.
- [x] Petición de documentación para cierre de proyecto.
- [x] Petición de informe de análisis de alertas.
- [x] Finalización de reuniones semanales

Decisiones tomadas

Aprobado: Se procede al cierre del proyecto. Entrega y reunión con el CISO para el cierre efectivo.

Aprobado: informe para el cierre de proyecto de operaciones que deben continuar y si es posible.

Aprobado: entrega de la documentación para cierre.

Requerido: informe de alertas preparado para el 08 Jun 2020

Aprobado: término de la presente reunión, se sustituirá por reuniones mensuales, además de reuniones de @ Daniel Rodríguez Fueyo con cada departamento.