Universidad de Buenos Aires Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Mejores prácticas para la implementación de un SIEM

Autor: Ing. Francisco Barreto

Tutor: Lic. Javier J. Vallejos Martinez

Presentación año 2025

Cohorte 2022

Declaración Jurada de origen de los contenidos:

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO

Francisco Barreto

DNI 33837580

Resumen

En el presente trabajo final de especialización se desarrolla el diseño e implementación de un Gestor de Eventos y Seguridad de la Información (SIEM por sus siglas en inglés, Security Information and Event Management) para una compañía genérica. El trabajo fue llevado a cabo en un entorno de virtualizado donde se configuraron y desplegaron componentes triviales y fundamentales para una infraestructura de seguridad, como un firewall, un IDS, un IPS, un Proxy y un controlador de dominio.

El objetivo principal es proporcionar una guía práctica y detallada que aborde los aspectos clave a considerar al implementar un SIEM en un entorno corporativo, abordando tanto en la configuración técnica como en los casos de uso más relevantes para una organización. Además, se detallan los escenarios más comunes, destacando cómo pueden aplicarse en situaciones empresariales reales para mejorar la detección y respuesta ante incidentes de seguridad.

Para cumplir con este propósito, se desarrolló un laboratorio práctico que simula un entorno corporativo, permitiendo evaluar la efectividad de diversas configuraciones y estrategias de seguridad implementadas.

Índice

Introducción

Contexto y antecedentes

La pandemia de COVID-19 marcó un punto de inflexión en la manera en que las compañías operan a nivel global, obligándolas a realizar una transición masiva y acelerada hacia entornos de trabajo remoto. Lo que en el pasado era considerado una modalidad opcional, reservada para roles específicos o circunstancias puntuales, se convirtió de manera repentina en una necesidad esencial para garantizar la continuidad operativa en un contexto de confinamiento y distanciamiento social. Este cambio drástico no solo afectó la dinámica laboral, sino que también planteó desafíos significativos en el ámbito de la ciberseguridad.

A medida que las organizaciones adaptaban sus infraestructuras para permitir el acceso remoto, fue necesario implementar nuevas estrategias, herramientas y políticas de seguridad informática. El objetivo fue doble, garantizar que los empleados pudieran acceder a los recursos corporativos de manera segura y proteger la información crítica frente a las crecientes amenazas. Sin embargo, esta rápida transformación no estuvo exenta de dificultades. La ampliación de las superficies de ataque, la dependencia de redes domésticas y dispositivos personales, y el uso generalizado de tecnologías en la nube generaron un entorno propicio para los ciberataques.

El incremento de los incidentes de ciberseguridad durante este período fue notable, con ataques de phishing, ransomware y robos de credenciales [1]. Este escenario obligó a las compañías a redoblar esfuerzos e inversiones en soluciones de ciberseguridad. En particular, las grandes compañías adoptaron múltiples herramientas y sistemas para mitigar riesgos, tales como sistemas de detección y respuesta de amenazas (EDR, XDR), firewalls y soluciones de autenticación multifactor.

No obstante, la implementación de numerosas soluciones de ciberseguridad dio lugar a un nuevo desafío: la generación de un volumen masivo de alertas y notificaciones. Este fenómeno, conocido como alert fatigue o "fatiga de alertas"

[2], dificultó el seguimiento efectivo de las amenazas, ya que los equipos de seguridad deben lidiar con la priorización y gestión de cientos o incluso miles de incidentes diarios. Este contexto pone de manifiesto la necesidad de desarrollar enfoques más integrados y automatizados que permitan optimizar la respuesta a incidentes, garantizar una protección efectiva y, al mismo tiempo, minimizar la sobrecarga para los profesionales encargados de la seguridad.

Propuesta

Una solución a este inconveniente es centralizar todas las alarmas de seguridad en un SIEM dado que nos permite concentrar todos los eventos de seguridad en un único lugar para analizarlos y tomar las acciones correspondientes de mitigación en los casos que sean necesarios. Pero solo con la adquisición de un SIEM no es suficiente, para implementarlo correctamente, es necesario realizar un análisis previo. Este análisis deberá abarcar los eventos y logs que queremos monitorear, los vínculos de comunicaciones necesarios, el volumen de eventos, el hardware requerido, las criticidades de las alarmas generadas y finalmente qué tratamiento se le darán a las mismas.

Además, es fundamental considerar la correcta configuración y correlación de eventos dentro del SIEM para optimizar su eficiencia y reducir la generación de falsos positivos. Esto implica definir reglas y umbrales adecuados, definir en conjunto con las áreas correspondientes procesos de respuesta ante incidentes y asegurar la integración con otras herramientas de seguridad como firewalls e IDS/IPS. Una implementación adecuada del SIEM no solo mejora la detección y respuesta ante amenazas, sino que también contribuye al cumplimiento de normativas y estándares de seguridad, fortaleciendo la postura de ciberseguridad de la compañía.

Objetivo

El objetivo del trabajo final de especialización es desarrollar un plan de estudio, análisis e implementación de un SIEM basado en diversas experiencias. Su implementación es crucial para obtener una visión integral de todos los productos de seguridad informática, lo que facilita una detección más efectiva de incidentes, así como su investigación y resolución cuando sea necesario.

Como parte de este objetivo también se busca implementar un entorno virtualizado que facilite la creación y gestión de múltiples máquinas virtuales, permitiendo simular la topología de red de una compañía. Una vez desplegado el entorno virtualizado, se demostrará la configuración de casos de uso contemplando desde la ingesta de los datos hasta la validación de la búsqueda y la recepción de alertas a través de correos electrónicos.

Metodología

Para implementar correctamente un SIEM, es esencial seguir una metodología rigurosa. Esta incluye un análisis exhaustivo de los eventos, logs a monitorear, evaluación de los vínculos de comunicaciones, el volumen de datos y la especificación del hardware necesario. Se deben clasificar los eventos según su criticidad, definir políticas de alerta, desarrollar procedimientos de respuesta a incidentes y capacitar al personal.

Lo anteriormente mencionado depende directamente del grado de madurez de la compañía. Una organización con procesos de seguridad más desarrollados podrá definir reglas de correlación más avanzadas y automatizar respuestas a incidentes, mientras que con una de menor madurez requerirá un enfoque progresivo, priorizando la visibilidad y la generación de alertas básicas.

Tras un despliegue inicial con sus correspondientes pruebas piloto, el SIEM deberá ser monitoreado y optimizado continuamente para asegurar su eficacia en la detección y la mitigación de incidentes de seguridad, manteniendo su resiliencia a nuevas amenazas o cambios en la infraestructura.

Marco teórico

Syslog

Syslog [3] es un protocolo estándar utilizado para enviar mensajes de registro o eventos del sistema a un servidor específico, denominado servidor syslog. Se utiliza principalmente para recopilar registros de dispositivos de máquinas diferentes en una ubicación central para su supervisión y revisión. El protocolo está habilitado en la mayoría de los equipos de red, como routers, switches, firewalls y otros dispositivos de red. Además, syslog está disponible en sistemas basados en Unix, Linux y en muchos servidores web. Syslog no está instalado por defecto en los sistemas Windows, estos utilizan su propio registro de eventos de Windows. Estos eventos pueden enviarse mediante utilidades de terceros u otras configuraciones que utilicen el protocolo syslog. Syslog se define en el RFC 5424, The Syslog Protocol, que dejó obsoleto el anterior RFC 3164. En cualquier dispositivo, el sistema genera varios eventos en respuesta a condiciones cambiantes, estos eventos suelen registrarse localmente donde pueden ser revisados y analizados por un administrador. Sin embargo, supervisar numerosos registros de manera individual en routers, switches y sistemas llevaría mucho tiempo y sería poco práctico. Syslog ayuda a resolver este problema mediante el reenvío de estos eventos a un servidor centralizado.

Transmisión de Syslog

Tradicionalmente, Syslog utiliza el protocolo UDP en el puerto 514, pero puede configurarse para utilizar cualquier puerto. Además, algunos dispositivos utilizan TCP 1468 para enviar datos syslog para obtener la confirmación de entrega del mensaje. La transmisión de paquetes syslog es asíncrona, lo que hace que se genere un mensaje syslog dentro del propio router, switch o servidor. El mensaje syslog consta de tres partes: PRI (un valor de prioridad calculado), HEADER (con información identificativa) y MSG (el mensaje en sí).

Formato de los mensajes syslog

Los datos PRI enviados a través del protocolo syslog proceden de dos valores numéricos que ayudan a categorizar el mensaje. El primero es el valor Facility que se puede observar en la Tabla 1 . Este valor es uno de los 15 valores

predefinidos o varios valores definidos localmente en el caso de 16 a 23. Estos valores categorizan el tipo de mensaje o qué sistema generó el evento.

Tabla 1. Syslog Message Facilities

Number	Facility description
0	Kernel messages
1	User-level messages
2	Mail System
3	System Daemons
4	Security/Authorization Messages
5	Messages generated by syslogd
6	Line Printer Subsystem
7	Network News Subsystem
8	UUCP Subsystem
9	Clock Daemon
10	Security/Authorization Messages
11	FTP Daemon
12	NTP Subsystem
13	Log Audit
14	Log Alert
15	Clock Daemon
16-23	Local Use 0 - 7

En la Tabla 2 se muestra una segunda etiqueta de un mensaje syslog donde clasifica la importancia o gravedad del mensaje en un código numérico de 0 a 7.

Tabla 2. Syslog Message Severities

Numerical Code	Code Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	Warning: warning conditions
5	Notice: normal but significant condition
6	Informational: informational messages
7	Debug: debug-level messages

Los valores de ambas etiquetas no tienen definiciones rígidas. Por lo tanto, depende del sistema o la aplicación determinar cómo registrar un evento (por ejemplo, como Informational o Error) y en qué servicio. Dentro de la misma aplicación o servicio, los números más bajos deberían corresponder a problemas más graves en relación con el proceso específico.

Los dos valores se combinan para producir un Valor de Prioridad que se envía con el mensaje. El valor de prioridad se calcula multiplicando el valor de la instalación por ocho y sumando el valor de gravedad al resultado. Cuanto menor sea el PRI, mayor será la prioridad.

(Valor de facilidad * 8) + Valor de gravedad = PRI

De este modo, un mensaje de núcleo recibe un valor inferior (mayor prioridad) que una alerta de registro, independientemente de la gravedad de la alerta de registro. Los identificadores adicionales del paquete incluyen el nombre del host, la dirección IP, el ID del proceso, el nombre de la aplicación y la marca de tiempo del mensaje.

El protocolo no define el contenido real del mensaje syslog. Algunos mensajes son texto simple y legible, otros pueden ser sólo legibles por la máquina. Los mensajes syslog no suelen superar los 1024 bytes.

Servidor Syslog

El servidor Syslog también se conoce como colector o receptor de syslog.

Los mensajes syslog se envían desde el dispositivo generador al colector.

Seguridad

El protocolo syslog no ofrece ningún mecanismo de seguridad. No incorpora autenticación para garantizar que los mensajes proceden del dispositivo que afirma enviarlos. No hay cifrado para ocultar la información que se envía al servidor. Es especialmente susceptible a los llamados "ataques de reproducción", en los que un atacante genera un flujo previo de avisos para obtener una respuesta.

Para remediar esta vulnerabilidad se puede utilizar cifrado TLS para mantener los mensajes de manera segura.

Limitaciones

Una limitación importante del protocolo syslog es que el dispositivo que se está supervisando debe estar en funcionamiento y conectado a la red para generar y enviar un evento syslog. Un error crítico de la instalación del núcleo puede que nunca envíe un error en absoluto, ya que, el sistema se desconecta. En otras palabras, syslog no es una buena forma de monitorear el estado el funcionamiento de los dispositivos.

SIEM

SIEM es una solución de seguridad que ayuda a las compañías a reconocer posibles amenazas y vulnerabilidades de seguridad antes de que tengan la oportunidad de interrumpir las operaciones comerciales. Otra función importante es mostrar anomalías en el comportamiento a nivel de usuario o direcciones IP automatizando muchos de los procesos manuales asociados con la detección de amenazas y la respuesta de incidentes, y se ha convertido en un elemento básico en los SOCs modernos para casos de uso de gestión de seguridad y conformidad [4].

Dentro de todas las funcionalidades que ofrece un SIEM, las más destacables son las siguientes:

- Unificar y gestionar logs: permitiendo centralizar los datos de diversas fuentes, almacenarlas, normalizarlas y dejarlas disponibles para realizar búsquedas eficientes.
- Cumplir con normativas vigentes: permite generar los controles necesarios para estar alineados con las diferentes normas, leyes o regulaciones que se exijan.
- Análisis forense: al centralizar y almacenar los datos de interés se obtiene la capacidad de realizar un análisis forense para determinar el origen de incidentes de seguridad.
- Responder de manera activa: al detectar un evento de seguridad que es considerado como un incidente y correlacionar con otros eventos, se puede tener mayor certeza de que sea un incidente de seguridad verdadero ayudando al analista de seguridad para tomar una decisión rápida y efectiva para su mitigación.
- Tablero para monitoreo: permite generar tableros para proyectar en un SOC.
- Presentación de informes: podemos generar informes tanto ejecutivos como técnicos según sea el destinatario.

Existen diferentes tipos de soluciones SIEM, en el siguiente cuadrante podemos visualizar los proveedores más reconocidos según la consultora de Gartner [5] como se puede observar en la Figura 1 .

Figura 1. Cuadrante Mágico de Gartner - SIEM 2022

Guía con prácticas recomendadas

Evaluación de necesidades

La implementación de TI requiere una planificación meticulosa, asegurando desde el inicio una comprensión clara de los objetivos de la compañía y de sus procesos clave. Este enfoque debe mantenerse durante todo el proceso de implementación, ya que, el SIEM está diseñado para asegurar la integridad, confidencialidad y disponibilidad de la información.

Una vez establecido el objetivo, es fundamental identificar las fuentes de datos que deben ser monitoreadas, analizadas y sobre las cuales se debe intervenir en caso de incidentes de seguridad. Una práctica común pero poco recomendada es enviar grandes volúmenes de registros y eventos al SIEM sin antes considerar qué tipo de información se está enviando y cómo será tratada, lo cual resulta en una recopilación innecesaria de información y un aumento de costos.

Después de identificar las fuentes de datos relacionadas con los procesos clave, es necesario determinar qué información de seguridad se enviará al SIEM para su monitoreo. Dado que es poco probable que seamos expertos en todas las fuentes de datos que se deben recolectar, es importante colaborar con los responsables de estas fuentes para obtener una comprensión más amplia.

Si la compañía cuenta con un nivel de madurez en Seguridad Informática, las políticas internas serán de gran ayuda para determinar qué información de seguridad monitorear y establecer los controles correspondientes. Además, la necesidad de cumplir con regulaciones o estándares específicos, como GDPR o SOX, también influirá en esta selección.

Por ejemplo, al monitorear eventos de seguridad en sistemas Windows, es esencial trabajar en conjunto con los administradores del dominio, quienes poseen el conocimiento especializado necesario para obtener información detallada. Este mismo enfoque debe aplicarse a todas las fuentes de datos que se desean monitorear.

Selección del SIEM adecuado

La selección de un SIEM adecuado reviste una importancia estratégica, uno de los primeros pasos cruciales en este proceso es estimar el volumen de logs o eventos que se van a analizar. Esta estimación es fundamental dado que afecta directamente al hardware necesario para la implementación y en algunos casos a las licencias requeridas para su funcionamiento.

Existen diferentes métodos para dimensionar la ingesta de logs en un SIEM. Dos de los enfoques más comunes son medir los EPS o los gigabytes por día. La elección del método adecuado dependerá de la solución específica que se vaya a implementar. Por ejemplo, Splunk, plataforma que utilizaremos en el laboratorio, utiliza el licenciamiento basado en gigabytes por día como métrica principal.

Además de considerar el volumen inicial de logs es importante evaluar la escalabilidad. También es fundamental la capacidad de adaptarse al crecimiento futuro de la compañía para garantizar una gestión de flujo creciente de eventos sin comprometer el rendimiento ni la eficacia.

Otro aspecto clave en la selección es la capacidad para integrarse con otras herramientas de seguridad, sistemas existentes en la infraestructura de la compañía, IPS, IDS, herramientas de análisis de vulnerabilidades y otros componentes esenciales para crear un ecosistema de seguridad unificado y efectivo.

Además de la propia tecnología, no se debe pasar por alto la importancia de la experiencia del usuario y el soporte técnico ofrecido por el proveedor del SIEM. Una interfaz intuitiva y fácil de usar puede agilizar las tareas de análisis y la respuesta ante incidentes.

Introducción a Splunk

Splunk es una plataforma de big data que simplifica la tarea de recopilar y gestionar volúmenes masivos de datos generados por máquinas y buscar información en ellos. La tecnología se utiliza para análisis web y empresarial, gestión de aplicaciones, cumplimiento y seguridad.

Las principales funciones son las siguientes:

Recopilación de datos: recopilar datos de diferentes fuentes, como archivos de registro, logs, bases de datos, aplicaciones web y sensores.

Indexación: los datos recopilados se indexan y estructuran para facilitar su búsqueda y análisis posterior. Dentro de Splunk se pueden crear índices de búsqueda optimizados para una recuperación rápida de información.

Búsqueda y consulta: los usuarios pueden realizar búsquedas poderosas y complejas en los datos indexados utilizando el lenguaje de consulta de Splunk SPL (Search Processing Language).

El SPL abarca todos los comandos de búsqueda y sus funciones, argumentos y cláusulas. Los comandos de búsqueda le dicen al software Splunk qué hacer con los eventos que recuperó de los índices. Por ejemplo, si debe utilizar un comando para filtrar información no deseada, extraer más información, evaluar nuevos campos, calcular estadísticas, reordenar los resultados o crear un gráfico. Algunos comandos de búsqueda tienen funciones y argumentos asociados con ellos. Estas funciones y sus argumentos sirven para especificar cómo actúan los comandos en sus resultados y en qué campos actúan. Por ejemplo, se puede utilizar funciones para formatear los datos en un gráfico, describir qué tipo de estadísticas calcular y especificar qué campos evaluar. Algunos comandos también utilizan cláusulas para especificar cómo agrupar los resultados de búsqueda.

Visualización y reportes: Splunk proporciona herramientas para crear visualizaciones gráficas y tabulares que ayudan a entender y presentar los resultados de las consultas.

Monitoreo y alertas: se utiliza para monitorear en tiempo real eventos y métricas específicas. Los usuarios pueden configurar alertas para recibir notificaciones cuando ciertos eventos o condiciones se cumplan.

Infraestructura de Splunk

Los principales componentes de Splunk son los siguientes [6]:

Forwarder: Es un componente que recopila datos de diversas fuentes y los envía al Indexer o a otros componentes de Splunk para su procesamiento y almacenamiento. Su función principal es actuar como un agente de envío de datos, facilitando la ingesta de datos.

Existen 2 tipos de Forwarders:

UF (Universal Forwarder): Es una versión ligera y eficiente del Forwarder que se utiliza para enviar datos a un Indexer o a un Heavy Forwarder. Los Universal Forwarders están diseñados para recopilar datos de múltiples fuentes, como registros de eventos, archivos de registro, métricas de sistemas, etc. Luego, envían esos datos a los componentes de Splunk para su procesamiento y almacenamiento.

En la Figura 2 se detallan las opciones para Windows

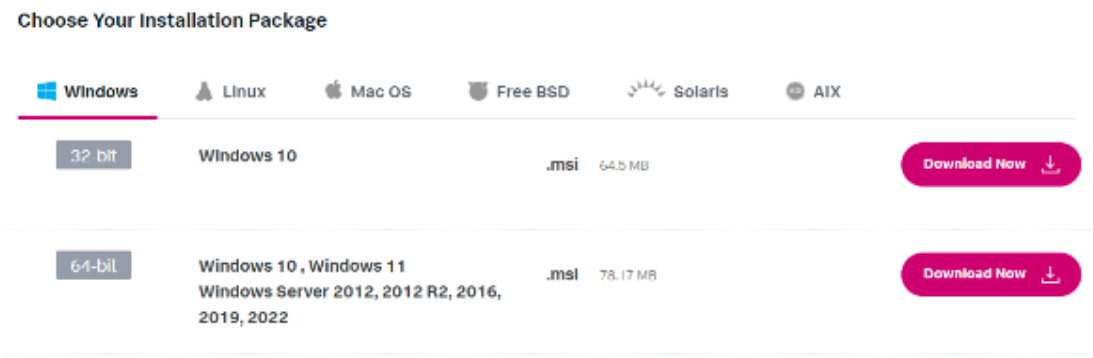


Figura 2 Universal Forwarders para Windows

En la Figura 3 se detallan las opciones para Linux

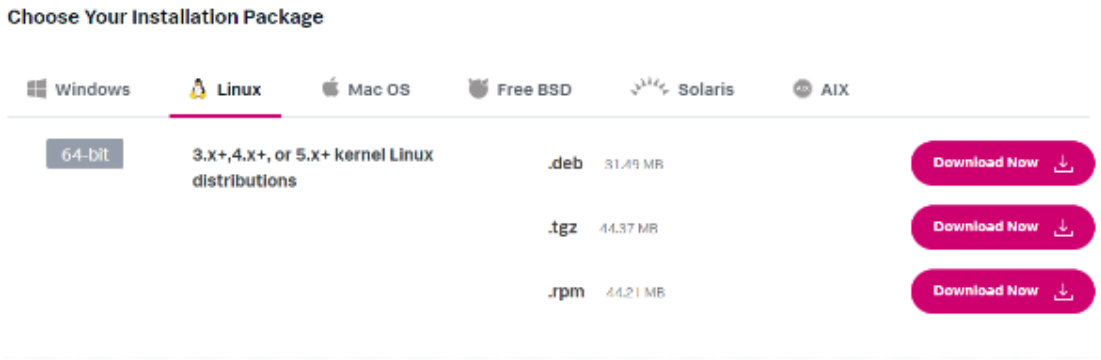


Figura 3 Universal Forwarders para Linux

HF (Heavy Forwarder): es una versión más potente y completa del Forwarder que puede realizar algunas tareas adicionales de procesamiento antes de enviar los datos al Indexer o a otros sistemas externos. Los Heavy Forwarders son capaces de aplicar transformaciones y filtrado a los datos antes de su envío, lo que permite una mayor flexibilidad y personalización en la recopilación y envío de datos.

Indexer: es uno de los componentes principales de la arquitectura que se encarga de recibir, almacenar e indexar los datos recopilados por los Forwarders. Su función principal es almacenar los datos en un formato optimizado para permitir búsquedas rápidas y eficientes, creando índices que facilitan la recuperación de información específica dentro de los datos.

Search Head: proporciona la interfaz de usuario y la funcionalidad para buscar, analizar y visualizar los datos indexados por los Indexers. Es el punto de entrada para que los usuarios interactúen con Splunk y obtengan información significativa a partir de los datos recopilados.

El Search Head tiene las siguientes funciones principales:

Interfaz de usuario: es la parte visible de Splunk para los usuarios finales. Proporciona una interfaz web intuitiva y fácil de usar donde los usuarios pueden ingresar consultas, realizar búsquedas complejas y ver los resultados.

Búsqueda y análisis: el Search Head permite a los usuarios buscar y analizar datos indexados por los Indexers. Los usuarios pueden utilizar el lenguaje de

búsqueda de Splunk (SPL) para formular consultas y obtener información relevante de manera rápida y efectiva.

Visualización y reportes: el Search Head permite a los usuarios crear visualizaciones gráficas, informes y paneles de control para presentar los resultados de las búsquedas y análisis de datos. Estas visualizaciones ayudan a los usuarios a comprender mejor los patrones y tendencias en los datos.

Administración de permisos: el Search Head también es responsable de gestionar los permisos de acceso a los datos y funciones de los usuarios. Permite establecer roles y permisos para controlar qué datos y funcionalidades pueden acceder diferentes usuarios.

El despliegue más simple es el que se obtiene por defecto cuando se instala por primera vez Splunk Enterprise en una máquina: una instancia independiente que se encarga tanto de la indexación como de la búsqueda.

Con esta configuración uno puede iniciar sesión en Splunk Web o la CLI en la instancia y configurar entradas de datos para recopilarlos. En la Figura 4 se detalla la arquitectura utilizada.

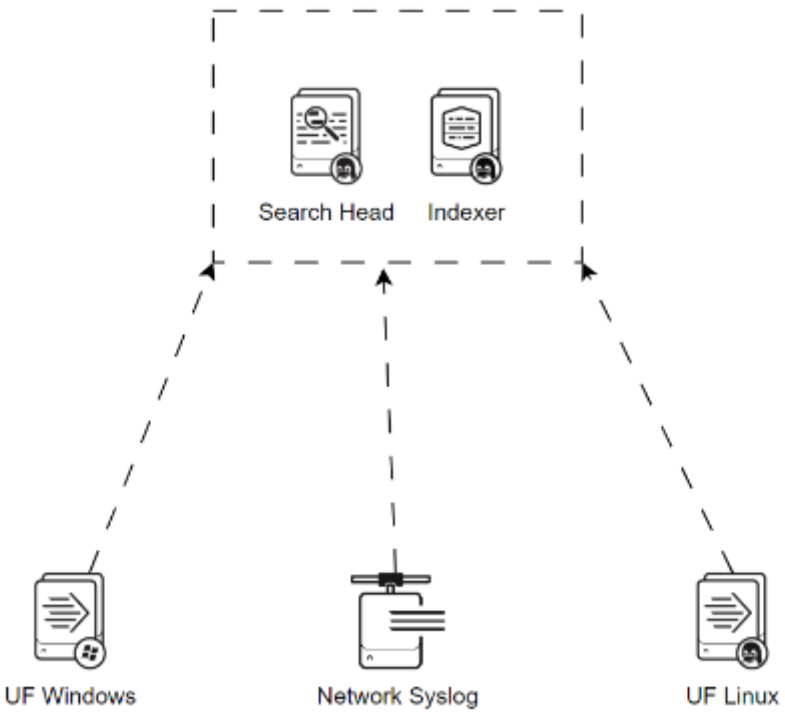


Figura 4 Arquitectura Splunk

Como se mencionó previamente, en la solución de Splunk existen UF dedicados para enviar los eventos de seguridad que configuremos en cada dispositivo.

En un principio deberíamos tener un UF por cada dispositivo a monitorear, pero si consideramos como ejemplo una compañía que posee 500 hosts Windows y 100 dispositivos que reportan mediante syslog los eventos; deberíamos tener 500 UFs instalados y configurados para reportar a Splunk, y de la misma manera deberíamos tener 100 envíos de syslog a Splunk.

Pero existen soluciones para obtener la misma información en Splunk pero de una manera más eficiente y escalable.

Para el caso de Windows la manera más efectiva y escalable es recopilar todos los eventos de Windows de un sistema a través de un concentrador. Windows Event Collector utiliza el protocolo Windows Remote Management (WinRM) para permitir el registro centralizado. En términos simples, Windows Event Collector proporciona un método nativo de Windows para centralizar los tipos de registros que puede capturar en Windows Event Viewer localmente [7].

Los recopiladores agregan registros de eventos de uno o más ordenadores de origen basándose en suscripciones a eventos. Existen dos tipos de suscripciones iniciadas por el origen e iniciadas por el recopilador. Las suscripciones iniciadas por el origen son más escalables porque puede configurarlas mediante una directiva de grupo sin conocer de antemano los orígenes específicos. El recopilador de eventos admite HTTP de texto sin formato y HTTPS cifrado para el envío de registros desde un origen a un recopilador.

De esta manera solo se instala un UF en el concentrador de Windows para luego reenviar los logs de todos los equipos del dominio a Splunk.

Respecto a los mensajes de syslog también es recomendable concentrarlos en un servidor, para ello Splunk recomienda hacerlo mediante Syslog-ng [8].

Planificación de la implementación

Es crucial contar con un plan de implementación sólido en el que todas las áreas involucradas tengan pleno conocimiento y se sientan partícipes, lo que contribuirá a fortalecer el compromiso de todo el equipo. A continuación, se detallarán las distintas fases de implementación:

Diseño: iniciar con un análisis detallado de los requisitos y objetivos de seguridad de la compañía. Esto incluye la identificación de activos críticos, las amenazas potenciales, las regulaciones que deben cumplirse y los casos de uso del SIEM.

Diseñar la arquitectura del SIEM, incluyendo la ubicación de los sensores de recolección de datos, los servidores de almacenamiento y análisis, la infraestructura y conectividad de red necesaria.

Definir los roles y responsabilidades de las áreas que intervienen en la implementación, así como los procedimientos para la gestión y respuesta de incidentes.

Implementación: considerando los plazos de tiempo disponibles con las áreas involucradas, la disponibilidad de hardware y licencias, se configura la infraestructura de hardware y software de acuerdo con el diseño establecido. Este proceso abarca desde la instalación hasta la normalización de servidores, la configuración de sensores para la recolección de datos, el establecimiento de canales de comunicaciones, y la implementación de copias de seguridad automáticas para cada plataforma instalada. Esta estrategia asegura la disponibilidad de un rápido “rollback” en caso de inconvenientes durante la implementación.

Posteriormente, se llevan a cabo pruebas de integración para garantizar que todos los componentes del SIEM funcionen de manera óptima y se comuniquen eficientemente entre sí. Este proceso resulta crucial para asegurar una detección eficaz y una gestión confiable de amenazas y eventos de seguridad.

Además de las pruebas técnicas, se desarrollan y documentan procedimientos detallados de seguridad que serán aplicados. Estos procedimientos incluyen aspectos como la retención adecuada de registros, la gestión efectiva de

incidentes de seguridad, y la definición de reglas de correlación de eventos para identificar patrones y comportamientos anómalos.

La documentación detallada de estos procedimientos no solo asegura una correcta implementación inicial, sino que también proporciona un marco sólido para el mantenimiento continuo y la optimización del SIEM en el tiempo.

Pruebas: es fundamental llevar a cabo pruebas exhaustivas de funcionalidad en el SIEM para garantizar su capacidad de recopilación, análisis y generación de alertas basadas en los datos de seguridad. Además de evaluar las funcionalidades en condiciones normales, es recomendable realizar pruebas que simulen contingencias. Por ejemplo, si el SIEM está configurado en un entorno de cluster con servidores, se debe verificar la continuidad del funcionamiento al indisponer uno de los servidores, así como comprobar la operatividad de canales de comunicación duplicados. Es esencial verificar que todas las redundancias disponibles actúen correctamente en caso de conmutación.

Además, se debe verificar que todos los servicios inicien automáticamente frente a reinicios de los servidores. Asimismo, es necesario llevar a cabo pruebas de rendimiento para evaluar la capacidad del SIEM para gestionar cargas de trabajo intensivas y para responder de forma rápida y eficiente a eventos de seguridad.

Puesta en marcha, evaluación y mejoras: es fundamental asegurarse de que el SIEM esté configurado de acuerdo con los estándares de seguridad establecidos. Esto implica verificar regularmente la configuración para detectar posibles brechas o desviaciones que puedan comprometer la seguridad.

El éxito del SIEM depende en gran medida de la capacitación adecuada del personal que lo utilizará. Esto incluye la formación en la interpretación de alertas, la gestión efectiva de incidentes y la generación de informes significativos. La capacitación continua garantiza que el personal esté preparado para enfrentar las amenazas de seguridad de manera eficiente.

Establecer procedimientos sólidos de monitorización es esencial para asegurar el funcionamiento de manera efectiva a lo largo del tiempo. Esto implica la implementación de controles y alertas automatizadas, así como la revisión

regular de los registros y eventos para detectar anomalías o actividades sospechosas.

Obtener retroalimentación del personal y los usuarios es fundamental para identificar áreas de mejora y ajustar la configuración según sea necesario. Esta retroalimentación puede provenir de análisis de incidentes, encuestas de satisfacción del usuario y revisiones periódicas de rendimiento.

Recopilación de datos

Al determinar los tipos de datos que un SIEM recopiló, es fundamental tener en cuenta una variedad de fuentes, tales como registros de eventos de sistemas, registros de aplicaciones, y registros de seguridad de red, entre otros. Estos datos pueden provenir de diferentes componentes de la infraestructura tecnológica de una compañía, incluyendo servidores, dispositivos de red, aplicaciones, y sistemas de seguridad. Es crucial definir con precisión qué tipos de eventos se recolectarán, ya que, esto impactará directamente en la capacidad de análisis y detección de amenazas del SIEM.

Además, se debe considerar cuidadosamente la frecuencia con la que estos eventos son enviados al SIEM para evitar sobrecargar la plataforma o incurrir en costos excesivos de licenciamiento. La eficiencia en la recolección y el almacenamiento de datos es esencial para garantizar un funcionamiento óptimo del SIEM sin comprometer su rendimiento ni su capacidad de análisis.

Una buena práctica en la configuración del SIEM es centralizar la recolección de datos. Esto implica integrar todas las fuentes de datos relevantes a través de un sistema centralizado, lo cual simplifica el proceso de integración y asegura la consistencia en la calidad y el formato de los datos recolectados. Esta integración centralizada también facilita la administración y el monitoreo de la recolección de datos, permitiendo una respuesta más rápida y efectiva ante eventos de seguridad.

Configuración de alertas

Las alertas y notificaciones son elementos clave en un SIEM, ya que, permiten identificar de manera temprana eventos y actividades anómalas que podrían indicar una posible amenaza de seguridad. A continuación, se detallan los pasos y consideraciones importantes para configurar adecuadamente estas alertas:

Identificación de eventos críticos: es fundamental identificar qué eventos son considerados críticos para la seguridad de la compañía. Esto puede incluir intentos de acceso no autorizado, actividades sospechosas en sistemas críticos, cambios inesperados en la configuración de red, entre otros.

Definición de umbrales: establecer umbrales o criterios específicos que activen una alerta ante comportamientos fuera de lo esperado o considerados normales. Por ejemplo, configurar una alerta cuando se detectan más de tres intentos fallidos de inicio de sesión en un período corto de tiempo (fuerza bruta).

Contextualización de alertas: asegurarse de que las alertas generadas por el SIEM estén contextualizadas y sean comprensibles para el equipo de seguridad. Incluir información relevante como la fuente del evento, la criticidad, el usuario, dirección IP o dispositivo involucrado y cualquier otra información que facilite la respuesta.

Priorización de alertas: priorizar la atención de las alertas según la criticidad definida, de manera que el equipo pueda enfocarse primero en aquellas que representen un mayor riesgo o impacto potencial en la seguridad de la compañía.

Escalado de alertas: definir un proceso claro de escalado para las alertas, especificando quiénes son los responsables de manejar cada nivel de alerta y los pasos a seguir en caso de que una alerta requiera una acción inmediata.

Notificaciones en tiempo real: configurar notificaciones en tiempo real para cuando se activen las alertas configuradas. Estas notificaciones pueden ser enviadas por correo electrónico, mensajes de texto o a través de canales de comunicación interna.

Automatización de respuestas: considerar la posibilidad de automatizar respuestas a ciertas alertas mediante integraciones con soluciones de

seguridad. Por ejemplo, configurar una regla para bloquear automáticamente la dirección IP de un atacante después de detectar varios intentos de intrusión en un firewall. Para ello se debe tener un tiempo de pruebas y evaluación para evitar que falsos positivos generen indisponibilidades no deseadas.

Revisión y ajuste continuo: realizar revisiones periódicas de las alertas generadas por el SIEM para asegurarte de que están siendo efectivas y ajustar la configuración según sea necesario para minimizar falsos positivos y maximizar la detección de amenazas reales.

Capacitación del personal

La capacitación del personal es fundamental para garantizar que el equipo de seguridad pueda utilizar eficazmente el SIEM, interpretar las alertas y responder adecuadamente a los incidentes. A continuación, se detallan algunas actividades:

Entrenamiento en el uso del SIEM: proporcionar entrenamiento detallado sobre cómo utilizar la interfaz, realizar búsquedas de eventos, generar informes y gestionar alertas.

Interpretación de alertas y eventos: capacitar al personal para interpretar correctamente las alertas generadas por el SIEM, diferenciando entre eventos normales, anormales y posibles incidentes de seguridad.

Procedimientos de respuesta a incidentes: instruir al personal en la aplicación de los procedimientos específicos de respuesta a incidentes que involucren al SIEM, incluyendo la escalada de alertas, la recolección de evidencia y la notificación de incidentes.

Análisis de tendencias: estar al tanto de las tendencias de seguridad tanto dentro como fuera de la compañía, incluso en otros mercados, y elaborar informes a partir de los datos recopilados por el SIEM; permitiendo identificar áreas de mejora en la postura de seguridad de la compañía.

Al invertir en la capacitación del personal de seguridad en el uso efectivo del SIEM, se fortalece directamente la capacidad del equipo en proteger los activos de la compañía y responder de manera rápida y eficiente a las amenazas.

Monitoreo y análisis continuo

La gestión efectiva de la seguridad informática requiere una atención constante de las operaciones, mantenimiento y el análisis continuo de las plataformas utilizadas. En el caso particular de Splunk, esta atención se vuelve aún más crítica debido a la naturaleza dinámica de las amenazas cibernéticas, que evolucionan y se multiplican día a día.

Para asegurar la efectividad de Splunk como plataforma de seguridad, es imprescindible mantenerse al día con las últimas actualizaciones y parches de seguridad. Esto garantiza no solo el funcionamiento óptimo del sistema, sino también una respuesta rápida y efectiva ante posibles amenazas.

En este sentido, se recomienda llevar a cabo las siguientes acciones:

Monitoreo Continuo: desarrollar paneles de control personalizados en el SIEM para visualizar métricas clave de seguridad, como la cantidad de eventos detectados, origen geográfico de los incidentes, el nivel de alertas generadas y la tendencia de incidentes.

Crear reportes automatizados que resuman la actividad de seguridad, los incidentes detectados, las acciones tomadas y las tendencias a lo largo del tiempo.

Implementación de Análisis de Comportamiento: configurar análisis de comportamiento en el SIEM para identificar patrones anómalos en el uso de sistemas y la actividad de los usuarios.

Gestión de Eventos: procesar y categorizar los eventos de seguridad entrantes para priorizar la respuesta a incidentes de manera eficiente.

Evaluar la criticidad de cada evento y tomar medidas adecuadas según las políticas y procedimientos de seguridad establecidos.

Investigación de Incidentes: utilizar las capacidades de búsqueda avanzada de Splunk para investigar incidentes de seguridad de manera efectiva y generar informes detallados sobre las acciones tomadas.

Refinar las consultas de búsqueda para obtener resultados precisos y relevantes, optimizando así la eficiencia operativa.

Gestión de Incidentes y Mejora Continua: registrar cada paso tomado durante la respuesta a incidentes y aplicar un enfoque de mejora continua al monitoreo y análisis.

Mantener al día las actualizaciones y parches de seguridad en Splunk y utilizar herramientas de análisis de datos para identificar tendencias y patrones de ataque.

Gestión de Usuarios y Accesos: administrar proactivamente los roles y permisos de usuario en Splunk para garantizar el acceso solo a personas autorizadas. Analizar las tendencias de seguridad a lo largo del tiempo para identificar patrones y amenazas emergentes, y comunicar hallazgos a las partes interesadas.

Al seguir estas recomendaciones y mantener un enfoque integral en la gestión de la seguridad informática con Splunk, se aumenta la capacidad de detectar, responder y prevenir amenazas cibernéticas de manera efectiva en tiempo real, contribuyendo así a un entorno informático seguro y resiliente.

Laboratorio

Plataforma

Se utilizó la plataforma VirtualBox debido a su amplia adopción como herramienta de virtualización, permitiendo la creación y administración de varias máquinas virtuales dentro de un entorno de host. Esta elección se fundamentó en la versatilidad de VirtualBox, su compatibilidad con diversos sistemas operativos y el respaldo de una extensa comunidad de usuarios, lo que brinda soporte y acceso a recursos adicionales para el proyecto.

Máquinas virtuales

Para el despliegue de las máquinas virtuales se utilizó una computadora de escritorio con las siguientes especificaciones técnicas: sistema operativo Windows 10 Pro, procesador Intel(R) Core(TM) i5- 1400 de 11ª generación, 32 GB de memoria RAM y un disco SSD de 256 GB.

En la Figura 5 se pueden visualizar las máquinas virtuales en el entorno de Virtualbox y en la Tabla 3 el detalle de las mismas.

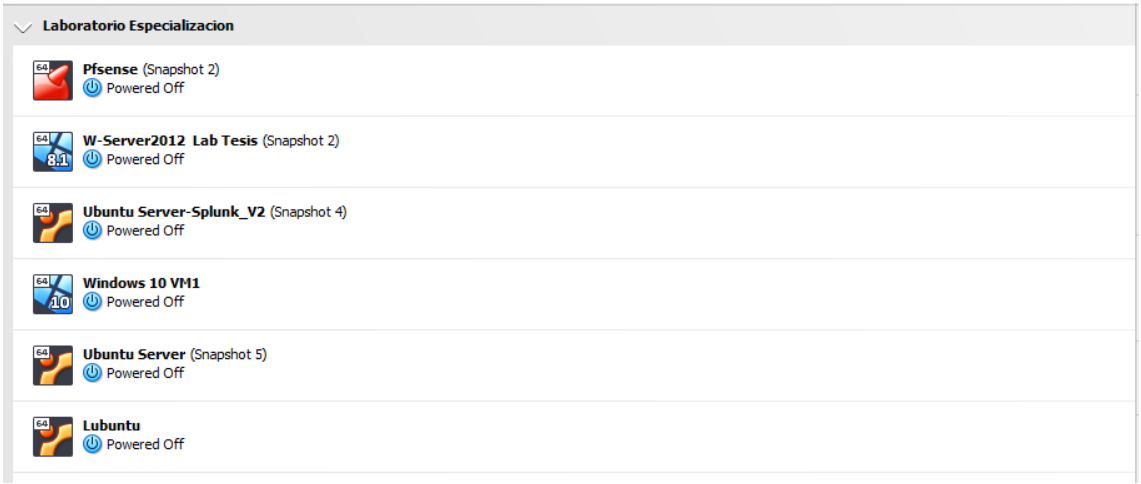


Figura 5 Máquinas Virtuales en Virtualbox

Tabla 3 Detalles Máquinas Virtuales

Maquina Virtual	Sistema Operativo	Recursos Asignados	Dirección IP	Función
PfSense	FreeBSD (64-bit)	4 GB de RAM, 16GB de almacenamiento, 4 vCPU	192.168.100.125 192.168.1.1	Firewall, DHCP, DNS, IDS y Proxy
W-Server2012 Lab Tesis	Windows server 20212 (64-bit)	6 GB de RAM, 40 GB de almacenamiento, 4 vCPU	192.168.1.21	Controlador de Dominio
Ubuntu Server-Splunk-V2	Ubuntu (64-bit)	6 GB de RAM, 80 GB de almacenamiento, 6 vCPU	192.168.1.10	Indexer y Search Head de Splunk
Windows 10 VM1	Windows 10(64-bit)	6 GB de RAM, 50 GB de almacenamiento, 6 vCPU	192.168.1.20	Gestión de PfSense, Splunk y Universal Forwarder Splunk
Ubuntu Server	Ubuntu (64-bit)	4 GB de RAM, 30 GB de almacenamiento, 2 vCPU	192.168.1.13	Pruebas Universal Forwarder Splunk
Lubuntu	Lubuntu (64-bit)	1 GB de RAM, 25 GB de almacenamiento, 1 vCPU	192.168.1.150	Pruebas y gestión de equipos

Topología y direccionamiento de red

Para el diseño de la topología y el direccionamiento de red, se utilizó la herramienta Drawio. En la Figura 6 , se puede observar la configuración empleada en el laboratorio.

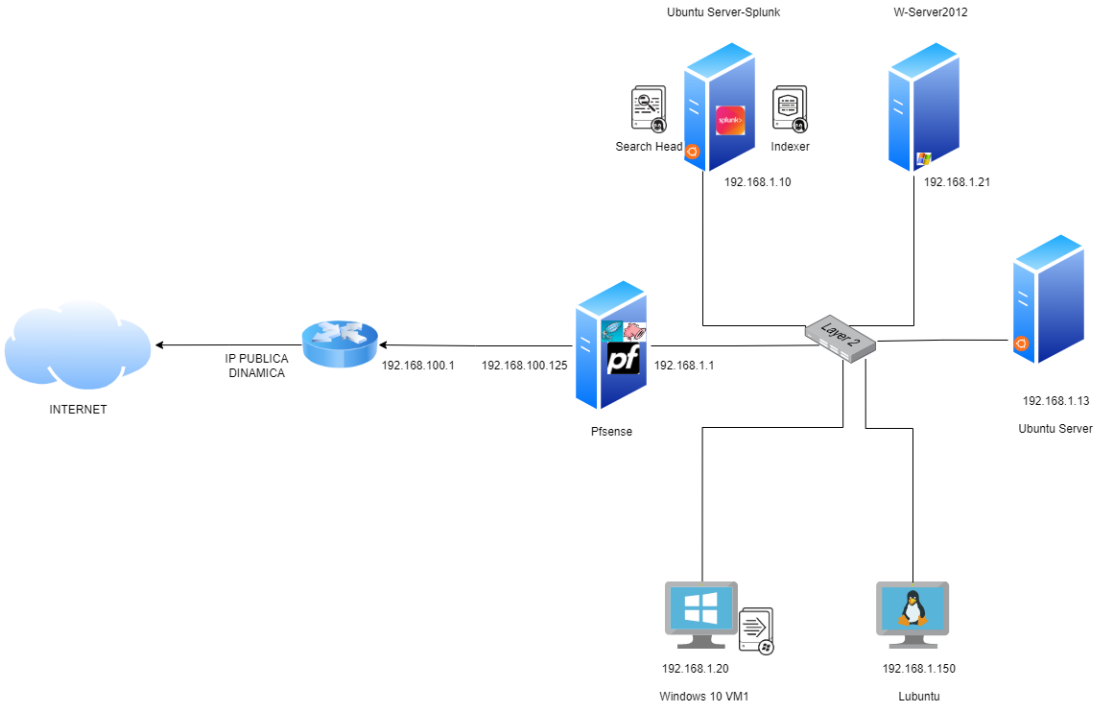


Figura 6 Topología y direccionamiento de red

Descripción del Laboratorio

En el laboratorio se utilizó el direccionamiento 192.168.1.0/24 y está compuesto por diferentes maquinas virtuales, cada una con roles específicos y ejecución de pruebas. A continuación, se detalla el rol y las características principales de cada VM utilizada:

pfSense

Es una distribución de software basada en FreeBSD, diseñada para actuar como un sistema operativo especializado en funciones de red. En este laboratorio cumple los siguientes roles esenciales:

- Router y Firewall:
    - Realiza la segmentación y el enrutamiento entre la red interna del laboratorio (192.168.1.0/24) y la red doméstica (192.168.100.0/24).
    - Permite crear y gestionar reglas de acceso, esenciales la generación de casos de uso.
- Servidor DHCP:
    - Configurado para asignar direcciones IP de manera dinámica facilitando la administración de dispositivos en la red.
- Servidor DNS:
    - Centraliza la resolución de consultas DNS del laboratorio.
- Sistema de Detección de Intrusos (IDS):
    - A través de la extensión Snort se implementan reglas para identificar y alertar sobre actividades sospechosas en la red.
- Proxy web:
    - A través de la extensión Squid se implementan filtros de navegación permitiendo la creación de los casos de uso correspondientes.

Windows Server 2012 (W-Server2012)

Este servidor cumple el siguiente rol:

- Controlador de Dominio (DC):
    - Gestiona los servicios de Active Directory, proporcionando autenticación centralizada para los usuarios y dispositivos del laboratorio.
    - Durante las pruebas, permite observar y comparar eventos generados por un servidor Windows frente a otros sistemas, como hosts con Windows 10 o servidores Linux

Ubuntu Server – V2

Basado en Ubuntu 22.04, esta configurado como el servidor principal de Splunk donde sus principales funciones son:

- Servidor Splunk:
    - Contiene el Indexer y Search Head de Splunk, componentes para recopilar, procesar y visualizar los datos provenientes de distintas fuentes.

Windows 10 (VM1)

Es una estación de trabajo que cumple diversos roles operativos y de pruebas:

- Gestor de soluciones:
    - Utilizada para administrar tanto las configuraciones de pfSense como las de Splunk.
- Pruebas de eventos:
    - Cuenta con un Universal Forwarder de Splunk, que recopila y envía eventos de Windows al servidor Splunk para su análisis.
    - Utilizada para simular eventos con el objetivo de validar los casos de uso.

Ubuntu Server

Basado en Ubuntu 22.04, tiene el mismo objetivo que la VM Windows 10 pero orientado a Linux con las siguientes funciones:

- Universal Forwarder:
    - Configurado para recolectar y enviar logs de eventos del sistema y de aplicaciones Linux hacia el servidor Splunk.
    - Facilita el análisis comparativo entre entornos Windows y Linux.

Lubuntu

Maquina virtual ligera con los siguientes roles:

- Pruebas de Navegación:
    - Permite realizar simulaciones de navegación web, evaluando políticas de filtrado de URLs implementadas en pfSense y otras configuraciones de seguridad.
- Validación de casos de uso:
    - Actúa como un cliente ligero para probar accesos y generar tráfico que puede ser monitoreado y analizado en Splunk.

Casos de uso

A continuación, se detallan 25 casos de uso relevantes para implementar en una compañía considerando las fuentes de datos utilizadas en el laboratorio:

Casos de uso referidos a Windows:

1) Detección de múltiples intentos de inicio de sesión fallidos en un host en un corto período de tiempo.
   a) Los intentos de inicio de sesión fallidos se registran en el Visor de Eventos, dentro de los Security Logs con el evento 4625. Detectar múltiples intentos fallidos en un corto período puede indicar ataques de fuerza bruta.
2) Detección de múltiples intentos fallidos de inicio de sesión desde un host hacia varios destinos en un corto período de tiempo.
   a) La detección de múltiples intentos fallidos de inicio de sesión desde un host hacia muchos destinos es importante porque podría indicar un ataque de fuerza bruta distribuido. Este tipo de ataque utiliza un único origen para probar credenciales en múltiples sistemas, intentando evadir bloqueos específicos por IP o alertas configuradas para un solo destino.
3) Detección de inicios de sesión fallidos desde un host utilizando credenciales con privilegios.
   a) La detección de intentos de inicio de sesión fallidos con credenciales privilegiadas es crítica, ya que estas cuentas suelen tener acceso administrativo o a datos sensibles. El evento 4625 en el Visor de Eventos registra intentos fallidos, destacando detalles como el nombre de la cuenta y el nivel de privilegios. Un atacante que utilice estas credenciales podría comprometer sistemas sensibles.
4) Detección de bloqueo de cuentas de usuarios privilegiados.
   a) La detección de bloqueo de cuentas de usuarios privilegiados es fundamental para identificar posibles intentos de acceso no autorizado, ya que estos usuarios no suelen tener un uso frecuente, y sus bloqueos pueden indicar un ataque dirigido. El evento 4740 (cuenta bloqueada), proporciona información sobre el nombre de usuario y la IP origen. Es importante correlacionar estos eventos con el origen de los intentos de inicio de sesión fallidos, para identificar patrones sospechosos.

5) Detección de bloqueo de cuenta de servicio.
    a) La detección de bloqueos en cuentas de servicio es crucial para asegurar la continuidad de los servicios críticos y detectar posibles intrusiones. El Evento 4740 de Windows registra el bloqueo de cuentas, siendo especialmente relevante para las cuentas de servicio, ya que estas no deben bloquearse con frecuencia.
6) Detección de eliminación de Registro de Eventos.
    a) La detección de la eliminación de registros de eventos es crucial para mantener la integridad de los registros de auditoría y detectar intentos de ocultar actividades maliciosas. La eliminación de registros de eventos se puede monitorear mediante el evento 1102, que indica cuando los registros del Visor de Eventos son borrados.
7) Detección de creación y eliminación de cuentas en un corto período de tiempo.
    a) La detección de cambios rápidos en las cuentas de usuario es crucial para identificar posibles intentos de evasión de seguridad, abuso de privilegios o brechas de seguridad. Los cambios sospechosos como la modificación de privilegios o la creación/eliminación de cuentas se registran con los siguientes eventos: 4720 (creación de una cuenta), 4722 (habilitación de una cuenta), y 4738 (modificación de una cuenta).

<u>Casos de uso referidos a Linux</u>

1) Detección de nuevos usuarios en servidores Linux donde no es frecuente su creación.
    a) La creación de nuevos usuarios en servidores donde esto no es una práctica común puede ser una señal clara de un intento de acceso no autorizado. Para detectar esta actividad se debe monitorear el archivo de registro /var/log/auth.log, que registra los eventos relacionados con la autenticación y la creación de usuarios. El comando useradd o cambios en el archivo /etc/passwd son clave, ya que se utilizan para crear nuevas cuentas.
2) Detectar incorporación de usuarios a grupos privilegiados como “sudo” o “wheel” en servidores Linux.

a) La detección de la incorporación de usuarios a grupos privilegiados como “sudo” o “wheel” en servidores Linux es esencial para garantizar que solo el personal autorizado tenga acceso a privilegios elevados. Los cambios en la membresía de estos grupos se pueden rastrear a través de los archivos /etc/group y /etc/sudoers, donde se gestionan los usuarios y sus permisos. La herramienta auditd se puede configurar para auditar la modificación de estos archivos, generando registros detallados sobre cualquier cambio.

3) Detección de eliminación de usuarios con privilegios Linux.
   a) La detección de la eliminación de cuentas con privilegios en servidores Linux es crucial para garantizar la trazabilidad y la integridad del sistema, ya que la eliminación de estas cuentas podría ser un indicio de un intento de encubrimiento de actividades maliciosas. Las eliminaciones de usuarios se registran en el archivo /var/log/auth.log, y comandos como userdel o deluser son comúnmente utilizados para borrar cuentas. La herramienta auditd puede configurarse para auditar estas operaciones y generar registros detallados.
4) Detección del borrado del archivo auth.log
   a) La detección de la eliminación del archivo auth.log es esencial para mantener la integridad de los registros de autenticación y evitar el encubrimiento de actividades maliciosas. Este archivo contiene eventos clave relacionados con los intentos de inicio de sesión, accesos y cambios en el sistema, y su eliminación puede indicar un intento de borrar evidencia de accesos no autorizados. Se pueden configurar herramientas como auditd para monitorear el acceso y la modificación de archivos críticos, incluyendo auth.log.
5) Detección de actividad root en horarios no laborales.
   a) Monitorear la actividad del usuario root fuera de los horarios laborales es esencial para identificar posibles accesos no autorizados o comportamientos anómalos que podrían comprometer la seguridad del sistema. Todas las acciones del usuario root, como la ejecución de comandos o cambios en configuraciones del sistema, quedan registradas en archivos de log como /var/log/auth.log o /var/log/secure.

Casos de uso referidos a FW pfSense

1) Tablero con la sumatoria de deny hacia internet
   a) La creación de un tablero que resuma los accesos denegados hacia Internet en pfSense es una herramienta clave para la detección de comportamientos anómalos y ataques potenciales. pfSense genera registros detallados de tráfico bloqueado en su Firewall Logs, específicamente a través de los eventos de tipo DENY.
2) Tablero con la sumatoria de allow hacia internet fuera del horario laboral.
   a) La visualización del tráfico permitido fuera del horario laboral permite identificar variaciones respecto a un comportamiento normal indicando actividades sospechosas.
3) Detectar asignación de nuevos usuarios con privilegios para la administración del FW.
   a) Detectar nuevos usuarios con privilegios para la administración permite controlar y prevenir futuros inicios de sesión.
4) Detección de múltiples intentos fallidos de inicio de sesión en la interfaz de administración en un breve período de tiempo.
   a) Monitorear los intentos fallidos de inicio de sesión en la administración de PfSense puede indicar intentos de fuerza bruta para comprometer el firewall.
5) Detección de tráfico hacia internet no permitido para hosts no autorizados.
   a) Identificar tráfico no autorizado hacia internet con los puertos UDP 53 (DNS), TCP 25 (SMTP), TCP 445 (SMB) TCP 465 (SMTPS), TCP 587 (SMTP STARTTLS), previene comunicaciones no autorizadas y posibles exfiltraciones de datos.

Casos de uso referidos a PfSense Squid

1) Monitorear el uso del ancho de banda
   a) Controlar y reportar el uso del ancho de banda por usuarios y aplicaciones asegura un uso eficiente de los recursos de red y detecta posibles abusos, optimizando así la performance de la red.
2) Detección de intentos de acceso a sitios web bloqueados

a) Identificar intentos de acceso a sitios web que han sido bloqueados por políticas de la compañía controla la implementación de las políticas de navegación y seguridad.

3) Detección accesos denegados a IOCs (indicadores de compromisos) webs declarados.
   a) Detectar accesos denegados permite identificar amenazas tempranas, evitar conexiones con sitios maliciosos y recopilar información crítica para análisis forense.

Casos de uso referidos a IDS Snort

1) Detección escaneo SYN:
   a) Monitorear y alertar sobre escaneos SYN para identificar puertos abiertos sin establecer conexiones completas detecta intentos de mapear la superficie de ataque.
2) Detección escaneo FIN:
   a) Monitorear y alertar sobre escaneos FIN permite identificar intentos de sondear puertos sin la intención de establecer conexiones completas, lo cual puede ser una técnica para evadir la detección por firewalls y sistemas de seguridad. Los escaneos FIN envían paquetes con el flag FIN activado a puertos de destino. Si el puerto está cerrado, el sistema de destino responderá con un paquete RST, mientras que, si el puerto está abierto no habrá respuesta.
3) Detección escaneo RST:
   a) Monitorear y alertar sobre escaneos RST ayuda a identificar intentos de interferir en comunicaciones existentes o descubrir puertos activos mediante la observación de las respuestas a paquetes RST inesperados. Los escaneos RST envían paquetes con el flag RST activado para intentar reiniciar conexiones TCP.
4) Detección escaneo XMAS Tree:
   a) Monitorear y alertar sobre escaneos XMAS Tree es crucial para detectar intentos complejos de sondeo, ya que estos paquetes tienen múltiples flags activados, lo cual puede provocar respuestas inusuales que revelen la presencia de puertos abiertos o vulnerabilidades específicas en sistemas de red.

5) Detección escaneo NULL:
    a) Monitorear y alertar sobre escaneos NULL permite identificar intentos de sondear puertos sin enviar datos (paquetes sin flags activados), una técnica utilizada para evadir ciertos mecanismos de detección. Los escaneos NULL envían paquetes sin ningún flag activado. Un puerto cerrado generalmente responderá con un paquete RST, mientras que un puerto abierto no responderá en absoluto. Esto permite a los atacantes identificar puertos abiertos sin generar demasiadas alertas en los sistemas de seguridad tradicionales.

De los 25 casos de uso mencionados se eligieron los 10 más relevantes que toda compañía debería implementar en primera instancia. Para cada uno, se expone inicialmente su objetivo, se detalla la configuración de detección y alerta, y se muestra cómo se presentará la alerta en un correo electrónico.

El Anexo 1 detalla la instalación y configuración de Splunk, los Universal Forwarders para Windows y Linux, y la configuración de casos de uso en ambos sistemas operativos.

Implementación casos de uso referidos a Windows

1) Detección de múltiples intentos de inicio de sesión fallidos en un host en un corto período de tiempo.
   a) Configuración en Splunk para realizar la búsqueda y alerta

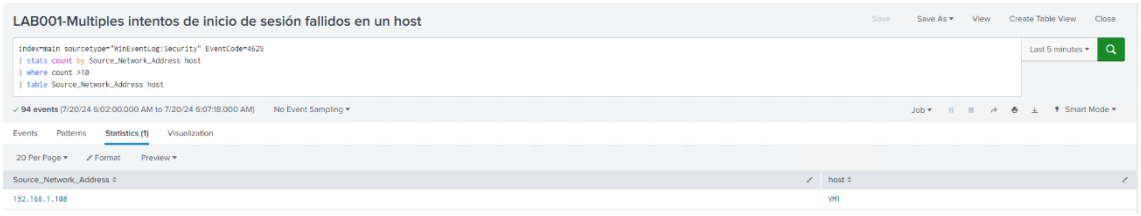


Figura 7 Búsqueda CU1

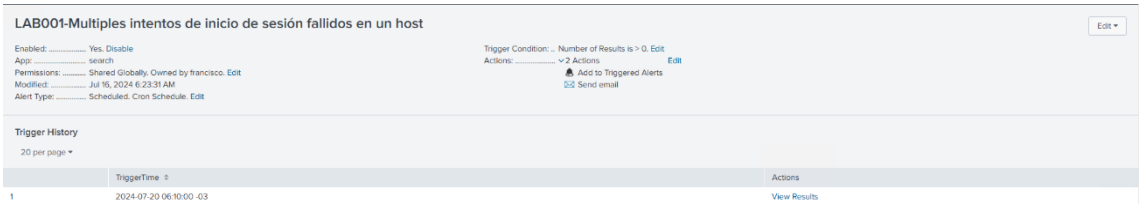


Figura 8 Alerta Splunk CU1

   b) Recepción de alerta por correo electrónico

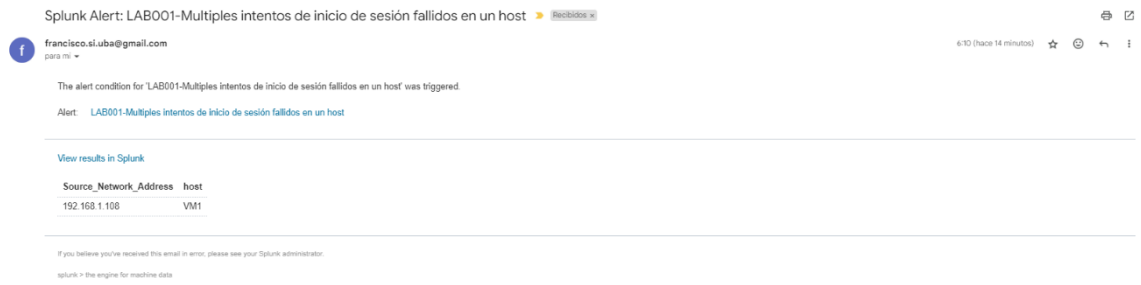


Figura 9 Alerta Correo CU1

2) Detección de múltiples intentos fallidos de inicio de sesión desde un host hacia varios destinos en un corto período de tiempo.

a) Configuración en Splunk para realizar la búsqueda y alerta

Figura 10 Búsqueda CU2

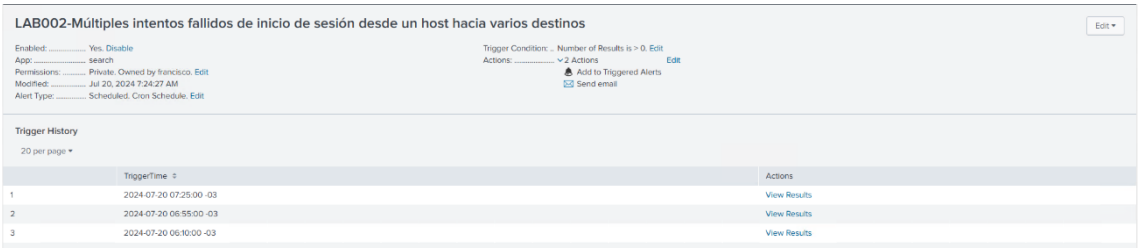


Figura 11 Alerta Splunk CU2

b) Recepción de alerta por correo electrónico

Figura 12 Alerta Correo CU2

3) Detección de inicios de sesión fallidos desde un host utilizando credenciales con privilegios

a) Configuración en Splunk para realizar la búsqueda y alerta

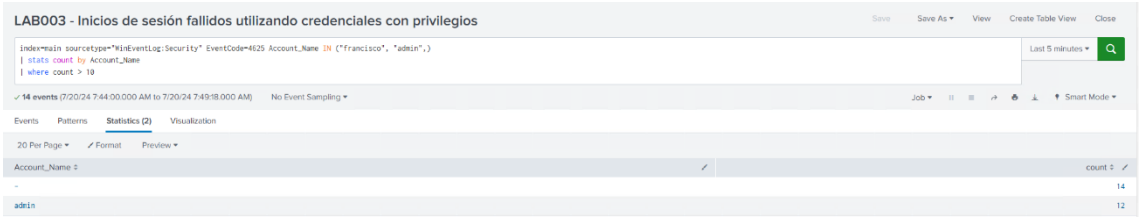


Figura 13 Búsqueda CU3

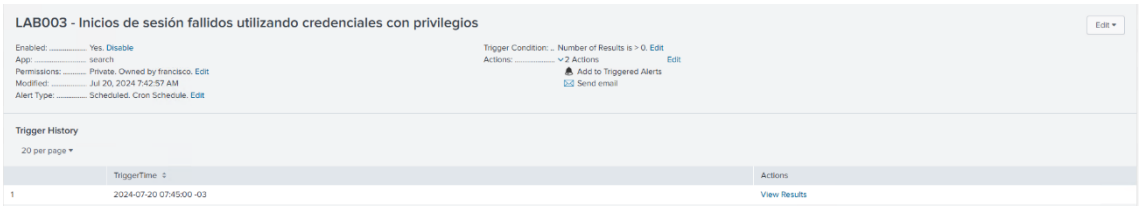


Figura 14 Alerta Splunk CU3

b) Recepción de alerta por correo electrónico

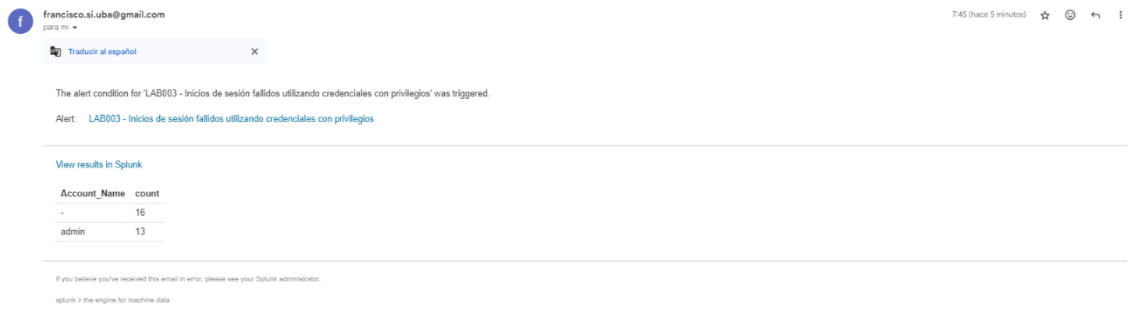


Figura 15 Alerta Correo CU3

4) Detección de eliminación de Registro de Eventos

a) Configuración en Splunk para realizar la búsqueda y alerta

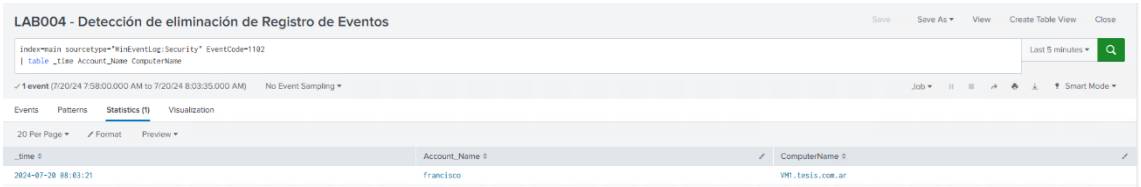


Figura 16 Búsqueda CU4

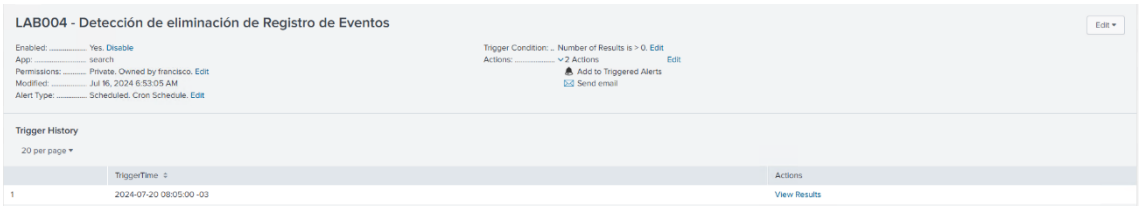


Figura 17 Alerta Splunk CU4

b) Recepción de alerta por correo electrónico

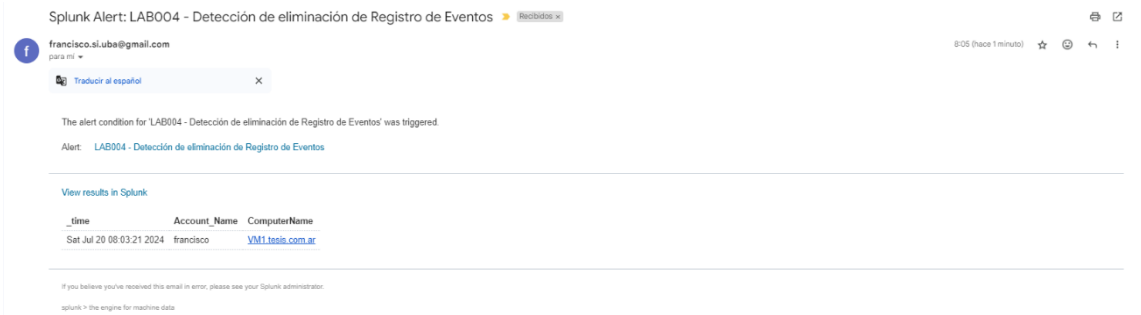


Figura 18 Alerta Correo CU4

Implementación casos de uso referidos a Linux

5) Detectar incorporación de usuarios a grupos privilegiados como “sudo” o “wheel” en servidores Linux.

a) Configuración en Splunk para realizar la búsqueda y alerta

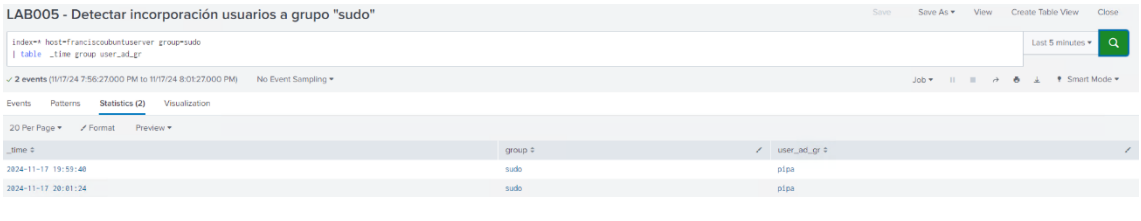


Figura 19 Búsqueda CU5

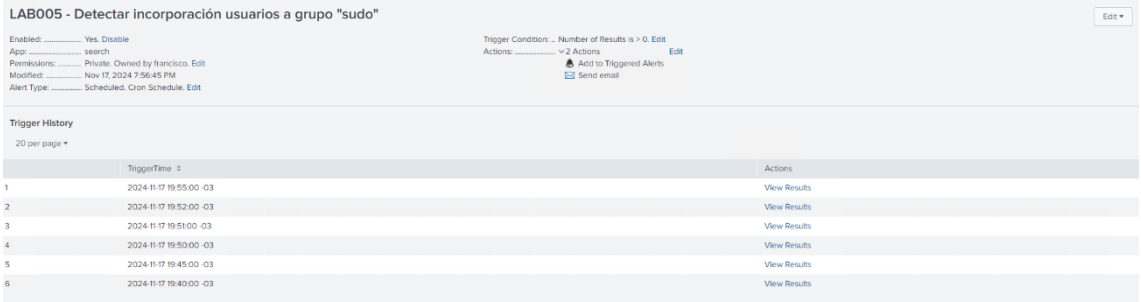


Figura 20 Alerta CU5

b) Recepción de alerta por correo electrónico

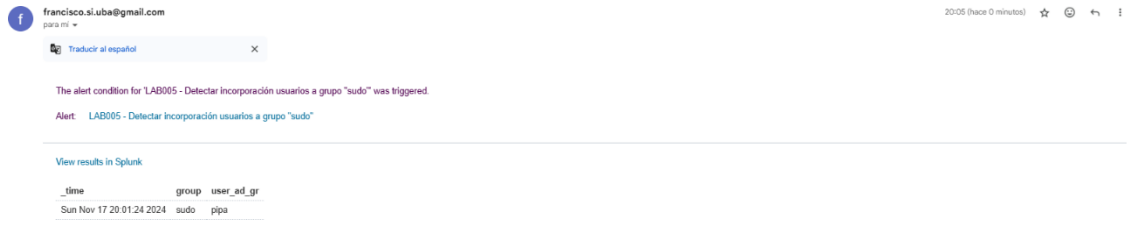


Figura 21 Alerta Correo CU5

6) Detección de eliminación de usuarios con privilegios Linux

a) Configuración en Splunk para realizar la búsqueda y alerta

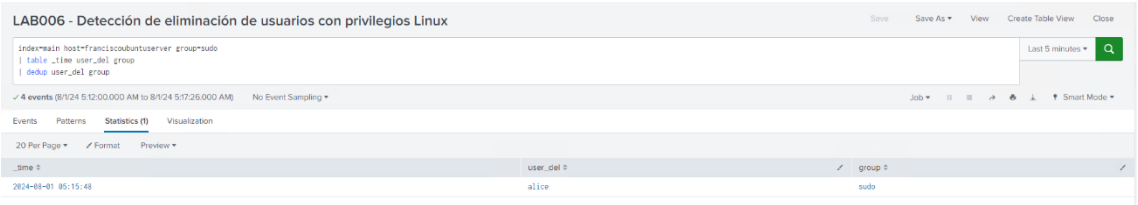


Figura 22 Búsqueda CU6

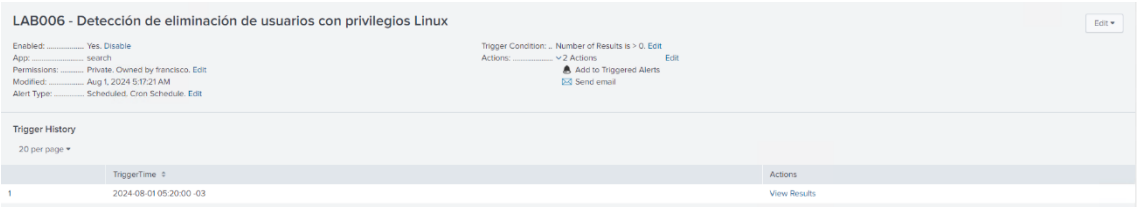


Figura 23 Alerta CU6

b) Recepción de alerta por correo electrónico

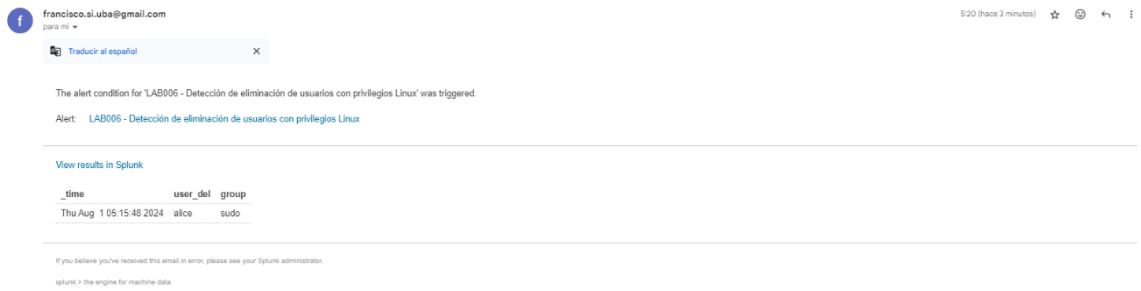


Figura 24 Alerta Correo CU6

7) Detección del borrado del archivo auth.log (habilitar el auditd)

a) Configuración en Splunk para realizar la búsqueda y alerta

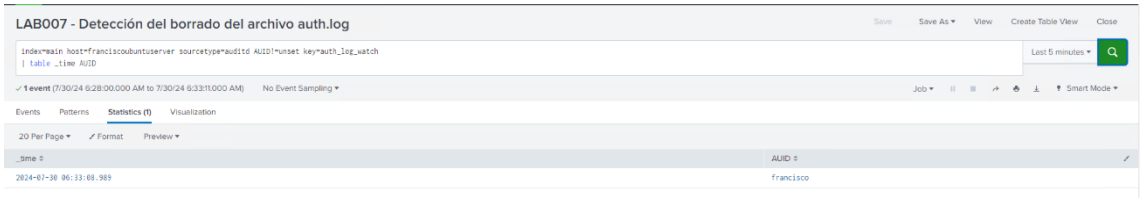


Figura 25 Búsqueda CU7

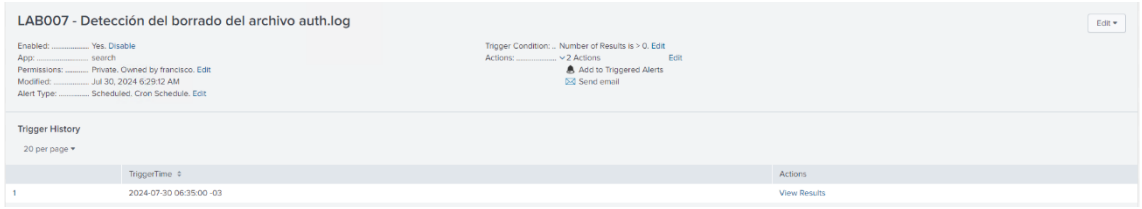


Figura 26 Alerta CU7

b) Recepción de alerta por correo electrónico

Figura 27 Alerta Correo CU7

Casos de uso referidos a FW PfSense

8) Tablero para monitoreo hacia internet
    a) Configuración en Splunk para realizar la búsqueda y tablero

Figura 28 Tablero Monitoreo PfSense

Implementación casos de uso referidos a PfSense Squid

9) Detección de intentos de acceso a sitios web bloqueados (hacking)
    a) Configuración en Splunk para realizar la búsqueda y alerta

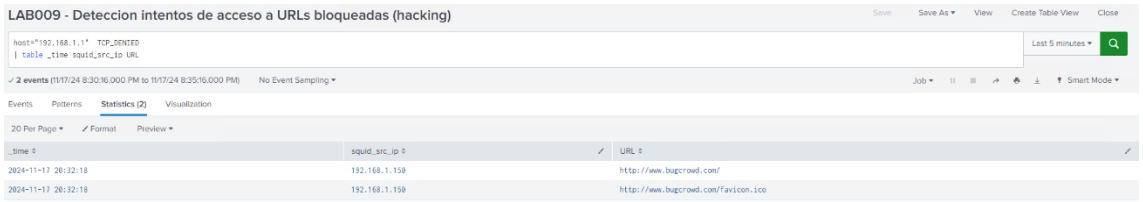


Figura 29 Búsqueda CU9

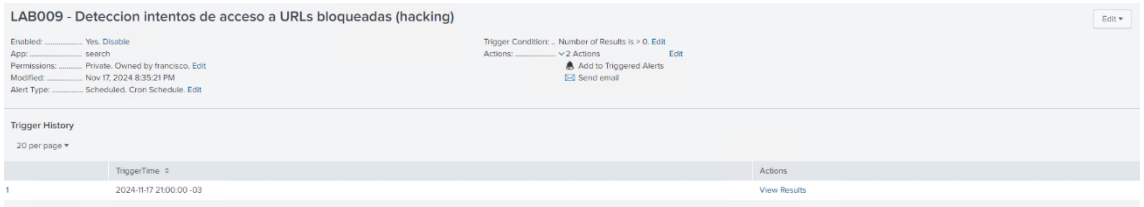


Figura 30 Alerta CU9

b) Recepción de alerta por correo electrónico

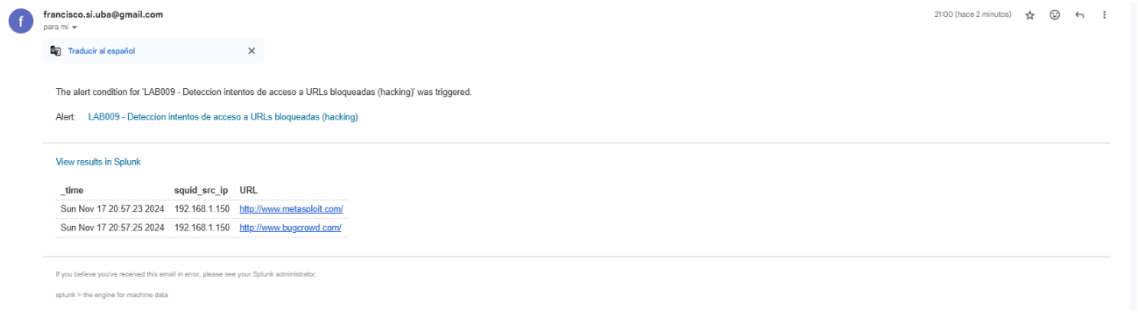


Figura 31 Alerta Correo CU9

Implementación casos de uso referidos a IDS Snort

10)Detección scan de TCP SYN

a) Configuración en Splunk para realizar la búsqueda y alerta

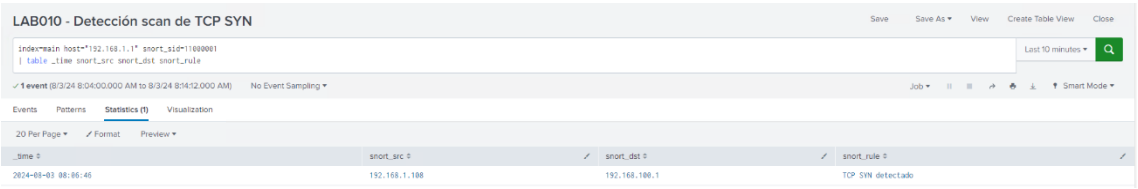


Figura 32 Búsqueda CU10

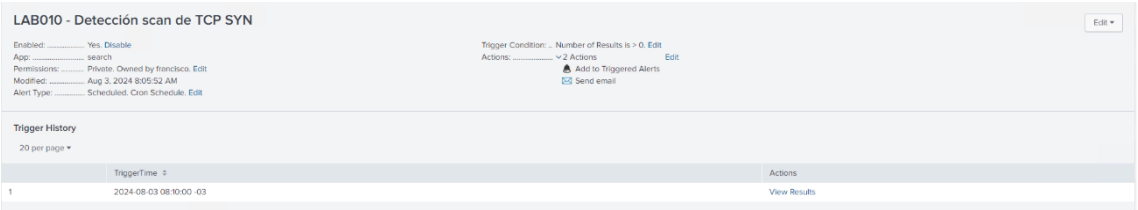


Figura 33 Alerta CU10

b) Recepción de alerta por correo electrónico

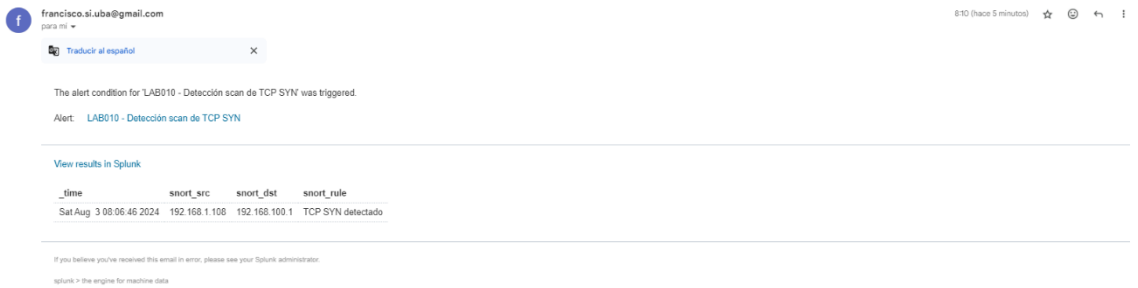


Figura 34 Alerta Correo CU10

Conclusiones

Resultados obtenidos

En el proceso de desarrollo del trabajo final de especialización se han destacado los puntos más importantes a considerar al momento de implementar un SIEM, abarcando todas las variables involucradas en su despliegue y funcionamiento. Este trabajo surge tanto de una investigación exhaustiva como de experiencias personales, anticipando posibles problemáticas y resaltando puntos clave a tener en cuenta. Aunque cada situación puede variar, ya sea en términos de las plataformas utilizadas, los tipos de datos utilizados u otros factores, el objetivo fundamental de implementar un SIEM es único: mejorar la capacidad para detectar y responder a incidentes de seguridad de manera eficiente, considerando la mayor cantidad de información de seguridad relevante. En el ámbito del laboratorio se llevó a cabo una demostración práctica de cómo sería la implementación de un SIEM, incluyendo la visualización de búsquedas y alertas generadas. Este enfoque práctico permitió demostrar de manera concreta los procesos y resultados esperados en un escenario real.

Futuras líneas de investigación

Al considerar mejoras y futuras líneas de investigación, se podría avanzar en los siguientes temas:

Simulación avanzada de amenazas:

Integrar herramientas de simulación avanzada de ataques en el entorno de laboratorio para evaluar la capacidad de detección y respuesta del SIEM frente a escenarios reales y complejos como ataques dirigidos.

Ampliación de fuentes de datos:

Exploración e implementación de casos de uso que utilicen una amplia variedad de fuentes de datos, incluyendo registros de aplicaciones web, logs de sistemas operativos móviles y datos de dispositivos IoT, para mejorar la detección de amenazas en entornos heterogéneos.

Correlación de eventos a gran escala:

Desarrollo de casos de uso y algoritmos de correlación que permitan analizar y correlacionar grandes volúmenes de eventos, aprovechando técnicas de análisis de big data y machine learning para identificar patrones de comportamientos anómalos y amenazas emergentes.

Desarrollo de tableros:

Creación e implementación de tableros personalizables que proporcionan una visión detallada del estado de seguridad, permitiendo a los analistas visualizar tendencias, métricas clave y alertas prioritarias de forma intuitiva y eficiente.

Automatización de respuesta a incidentes:

Automatizar búsquedas, detecciones y la respuesta a incidentes, para reducir la intervención humana y mejor los tiempos de respuesta. Esto incluye configurar reglas de acción automáticas y la integración con otros productos mediante una orquestación de seguridad.

Estas mejoras y líneas de investigación futuras buscan fortalecer la capacidad del SIEM para adaptarse a entornos dinámicos y complejos, mejorar la detección temprana de amenazas y facilitar la toma de decisiones para garantizar la seguridad y protección de los activos de la organización.

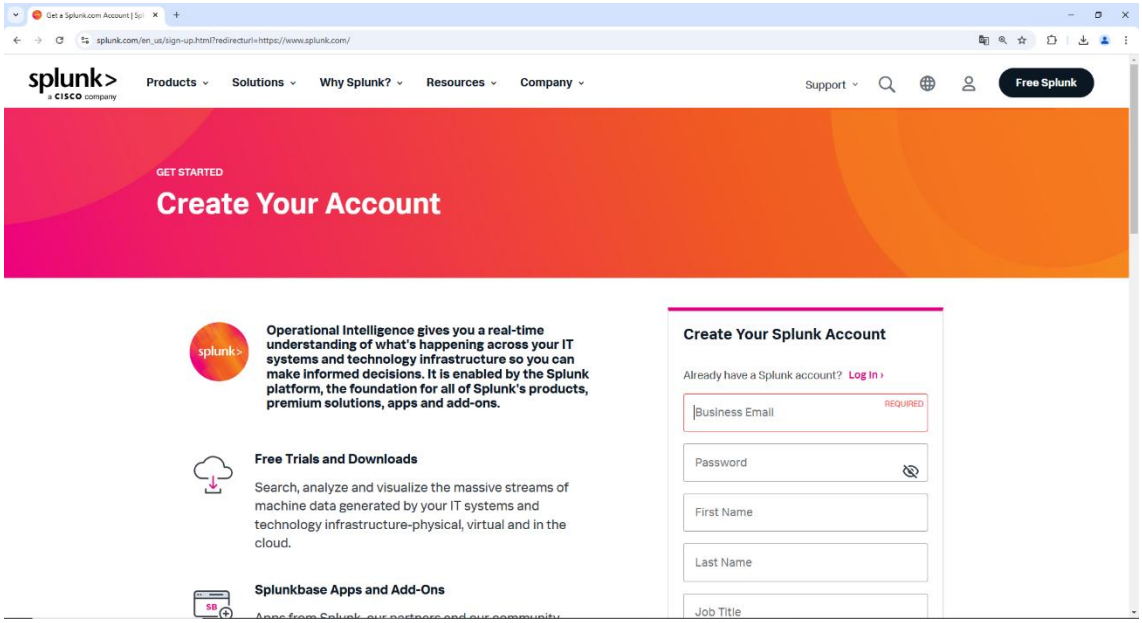
Glosario

- EDR (Endpont Detection and Response): herramienta que proporciona monitorización y análisis continuo del endpoint y la red
- XDR (Extended Detection and Response): herramienta que supervisa y mitiga las amenazas a la ciberseguridad.
- SIEM (Security Information and Event Management): gestión de eventos e incidentes de seguridad, este sistema se utiliza como correlacionador de eventos.
- IDS (Intrusion Detection System): sistema que detecta y alerta intrusiones o actividades maliciosas en tiempo real.
- IPS (Intrusion Prevention System): sistema que detecta y bloquea intrusiones o actividades maliciosas en tiempo real.
- Proxy web: servidor intermediario que filtra y gestiona el acceso a sitios web.
- SOC (Security Operation Center): centro de operaciones de seguridad para la prevención, detección y respuesta de amenazas.
- Firewall: dispositivo que controla el tráfico de red según reglas de seguridad.
- TI: tecnología de la información.
- EPS (Events Per Second): número de eventos analizables por segundo.
- SPL (Search Processing Language): es un lenguaje de procesamiento de búsqueda que se utilizan para consultar datos en Splunk.
- IOCs (Indicators of Compromise): es una pista o señal utilizada para identificar posibles amenazas o actividades maliciosas en un sistema o red.

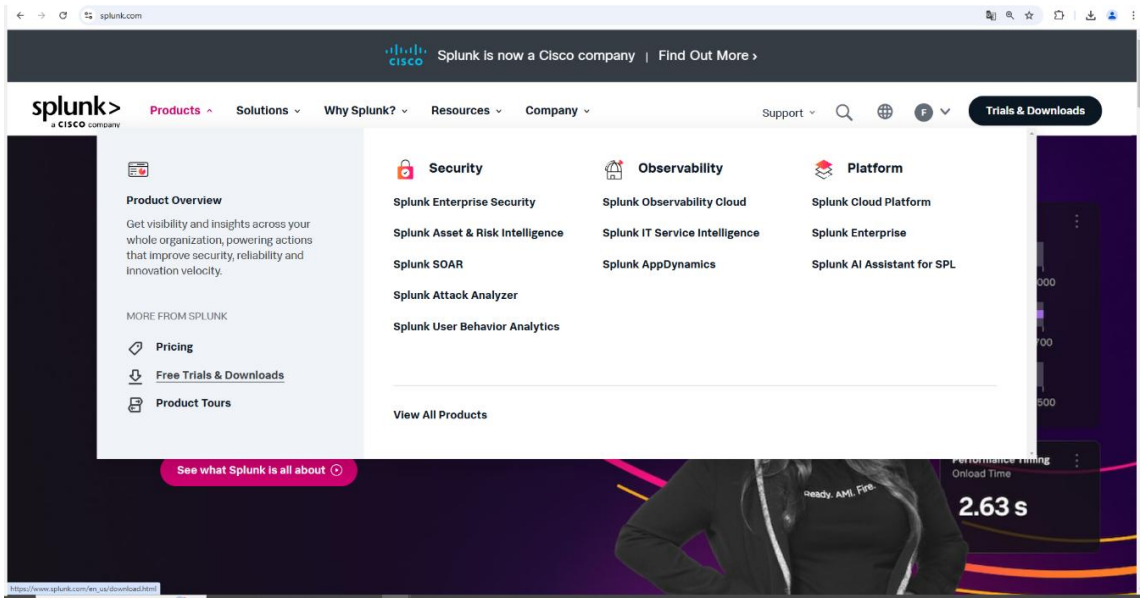
Anexo 1

Instalación de Splunk

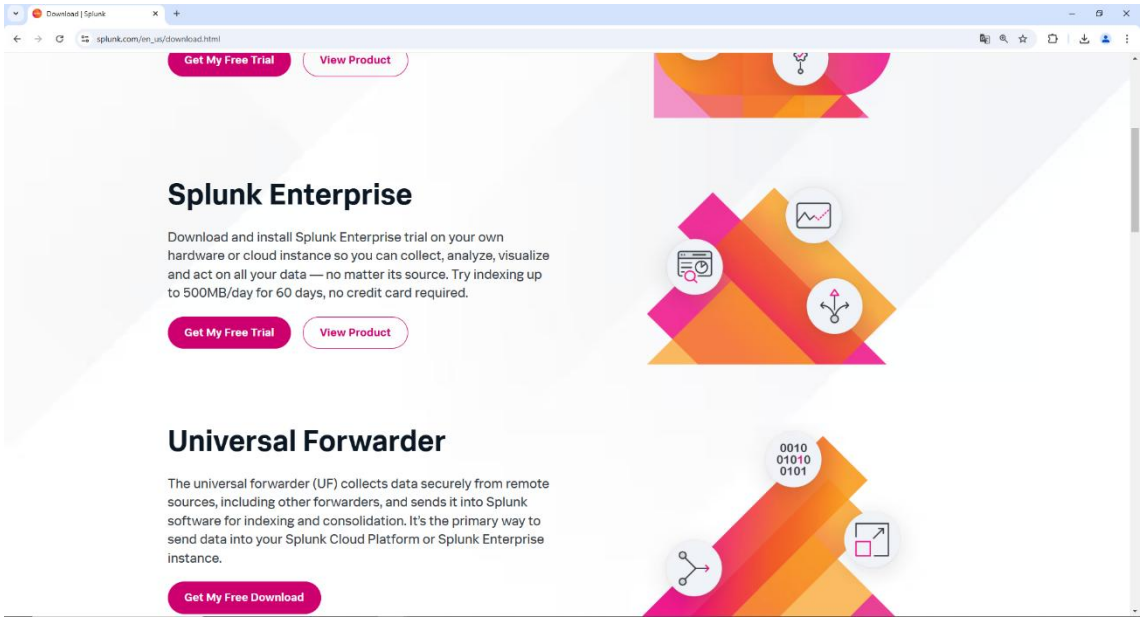
1. Ingresar a la página oficial de Splunk [9] y generar una cuenta para poder descargar los instaladores.



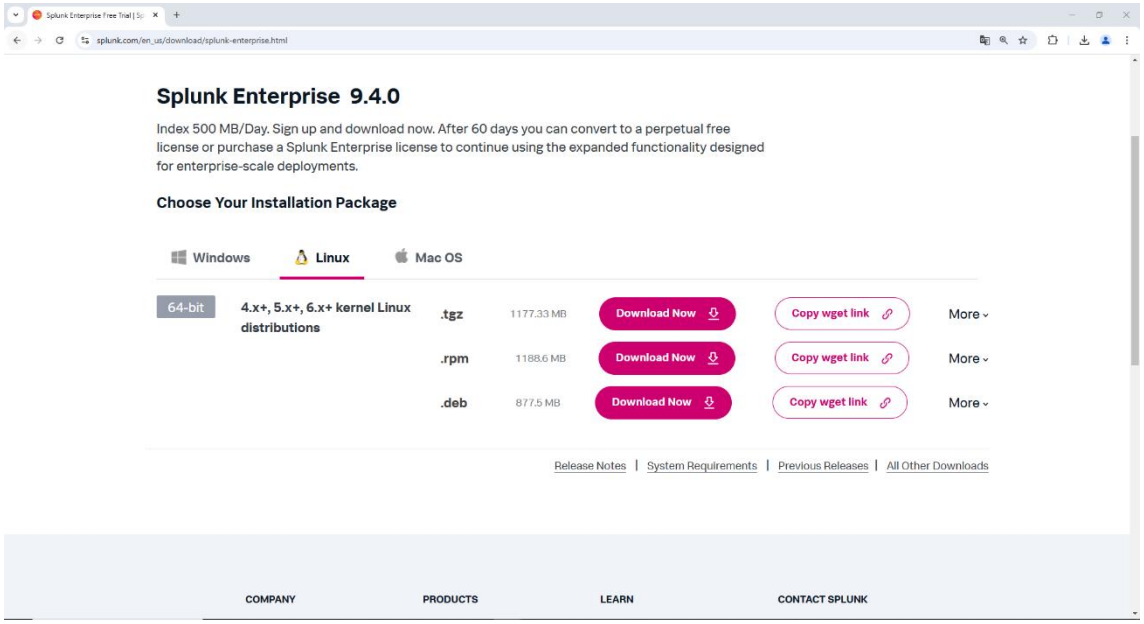
2. Una vez generadas las credenciales ingresar a “Free Trials & Download”.



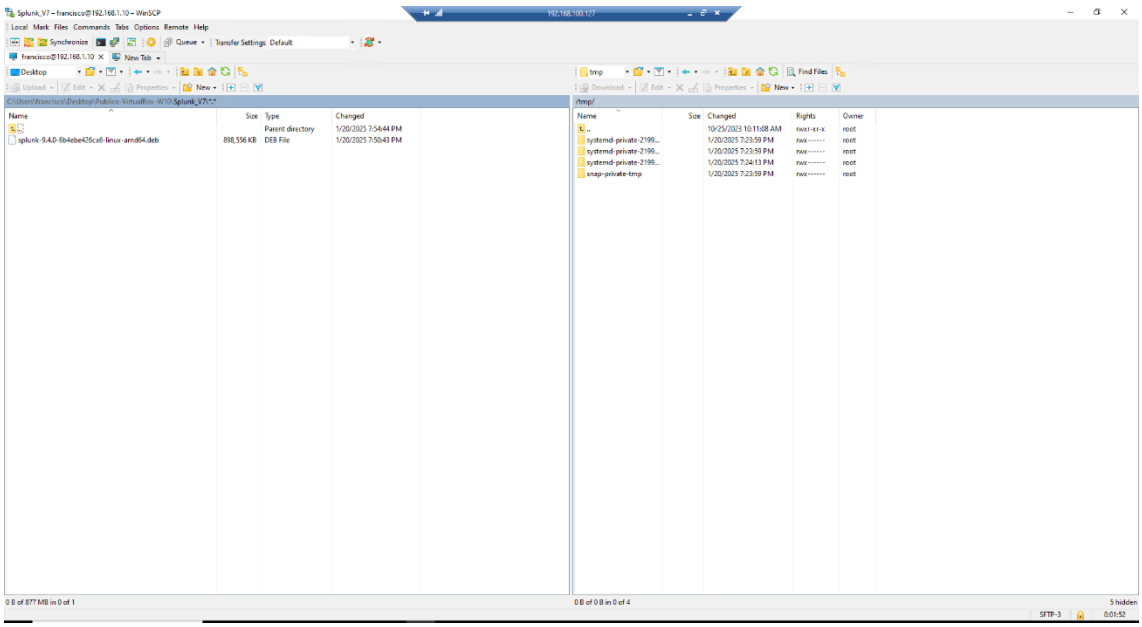
3. Seleccionar “Get My Free Trial”



4. En este caso instalaremos Splunk en un Ubuntu 22.04, por lo que descargaremos la versión 9.4.0 de Splunk para Linux 64-bit en formato .deb.



5. Copiar el instalador en el servidor en el directorio /tmp



6. Ejecutar el siguiente comando para instalar la instancia de Splunk:

sudo dpkg -i splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb

```
root@splunk-ubuntu:/tmp# dpkg -i s
snap-private-tmp/
splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb
systemd-private-51fd2008e366480d9cae42eec66429fa-systemd-logind.service-5iW5og/
systemd-private-51fd2008e366480d9cae42eec66429fa-systemd-resolved.service-Cvhx0j/
systemd-private-51fd2008e366480d9cae42eec66429fa-systemd-timesyncd.service-EEgOsd/
root@splunk-ubuntu:/tmp# dpkg -i splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb
Selecting previously unselected package splunk.
(Reading database ... 63903 files and directories currently installed.)
Preparing to unpack splunk-9.4.0-6b4ebe426ca6-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunk (9.4.0) ...
Setting up splunk (9.4.0) ...
complete
root@splunk-ubuntu:/tmp#
```

7. Para que Splunk se ejecute automáticamente después de que se inicie el servidor es necesario ejecutar el siguiente comando [10]:

sudo opt/splunk/bin/./splunk enable boot-start

Aceptar la licencia y generar usuario y password para administrar Splunk.

```
Do you agree with this license? [y/n]:          y
Do you agree with this license? [y/n]: y

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: francisco
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Copying '/opt/splunk/etc/openldap/ldap.conf.default' to '/opt/splunk/etc/openldap/ldap.conf'.
Generating RSA private key, 2048 bit long modulus
...+++++
.......+++++
e is 65537 (0x10001)
writing RSA key

Generating RSA private key, 2048 bit long modulus
.............................................................+++++
......................+++++
e is 65537 (0x10001)
writing RSA key

Moving '/opt/splunk/share/splunk/search_mrsparkle/modules.new' to '/opt/splunk/share/splunk/search_m
rsparkle/modules'.
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
root@splunk-ubuntu:/opt/splunk/bin# _
```

Verificar si el servicio está corriendo con el siguiente comando:

sudo ./splunk status

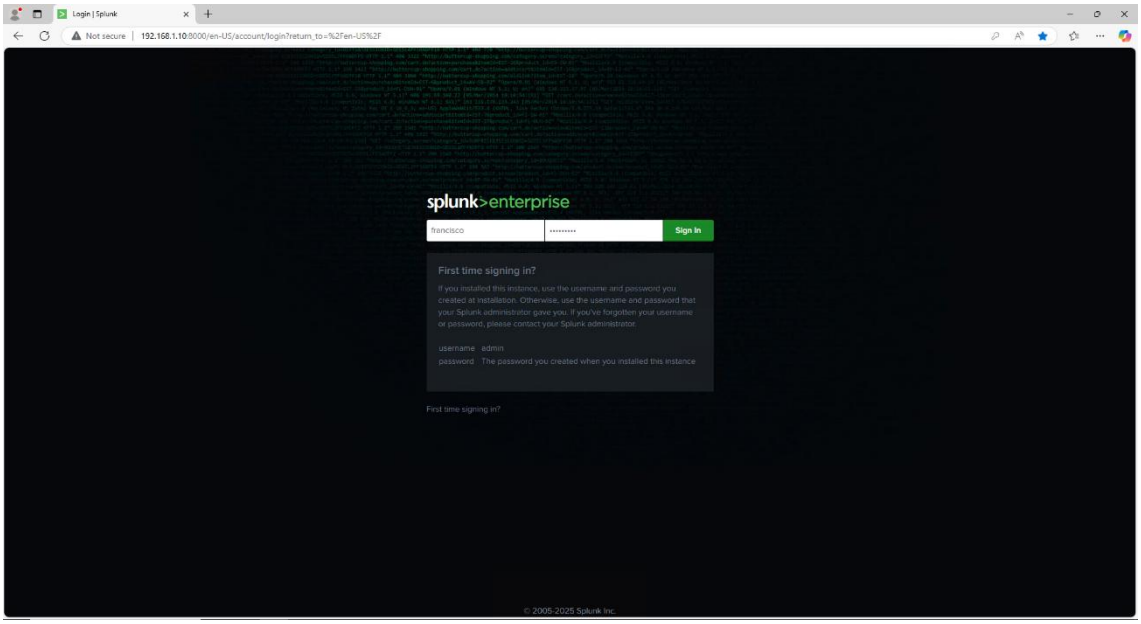
```
root@splunk-ubuntu:/opt/splunk/bin# ./splunk status
splunkd is not running.
root@splunk-ubuntu:/opt/splunk/bin# _
```

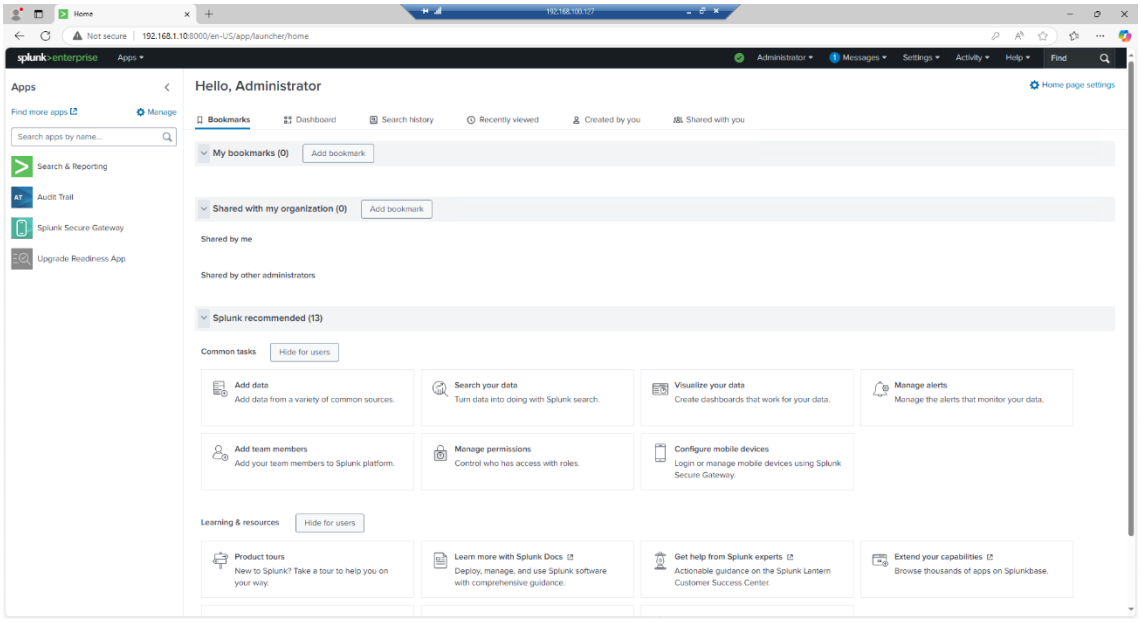
En el caso de no estar corriendo, ejecutar el siguiente comando:

sudo opt/splunk/bin/./splunk start

```
spection _metrics _metrics_rollup _telemetry _thefishbucket history main summary
        Done
        Checking filesystem compatibility...  Done
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunk/splunk-9.4.0-6b4ebe426ca6-linux-
amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Generating a RSA private key
.................+++++
........+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=splunk-ubuntu/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib
 and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased
 security
Done


Waiting for web server at http://127.0.0.1:8000 to be available..... Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://splunk-ubuntu:8000

root@splunk-ubuntu:/opt/splunk/bin# ./splunk start_
```

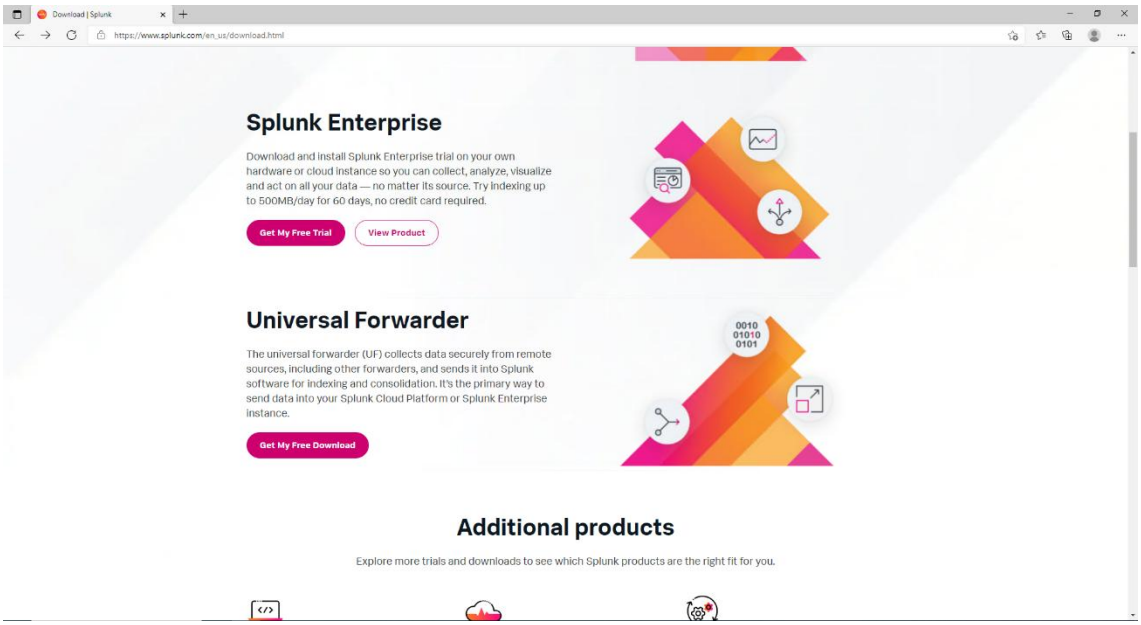
8. Con el servicio de Splunk iniciado, podemos ingresar a la interfaz web a través de la URL http://splunk-ubuntu:8000 utilizando las credenciales creadas en el paso anterior.
   En este caso es http://192.168.1.10:8000



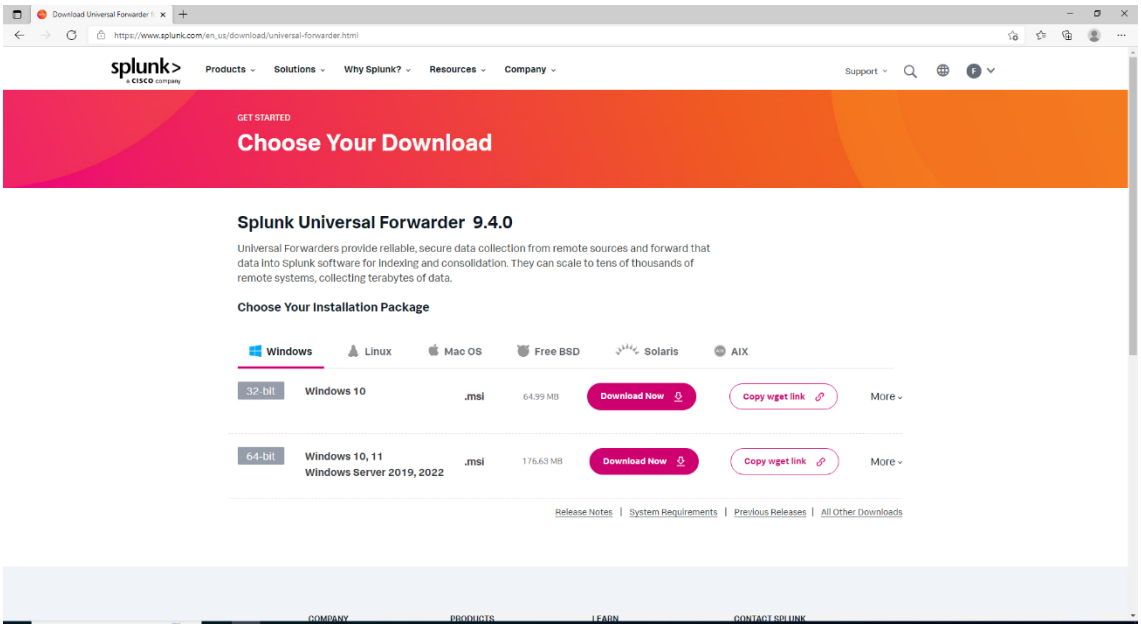


Instalación UF en Windows

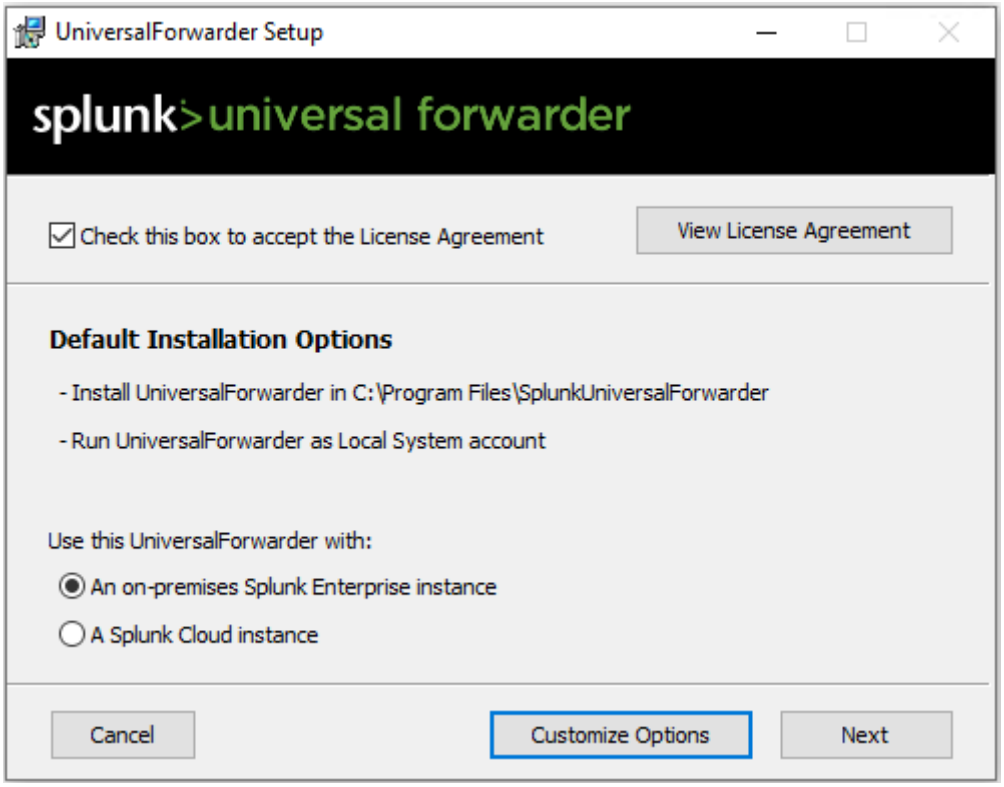
1. Para instalar el Universal Forwarder utilizaremos la documentación oficial de Splunk [11] Descargar el instalador del Universal Forwarder desde la página oficial de Splunk



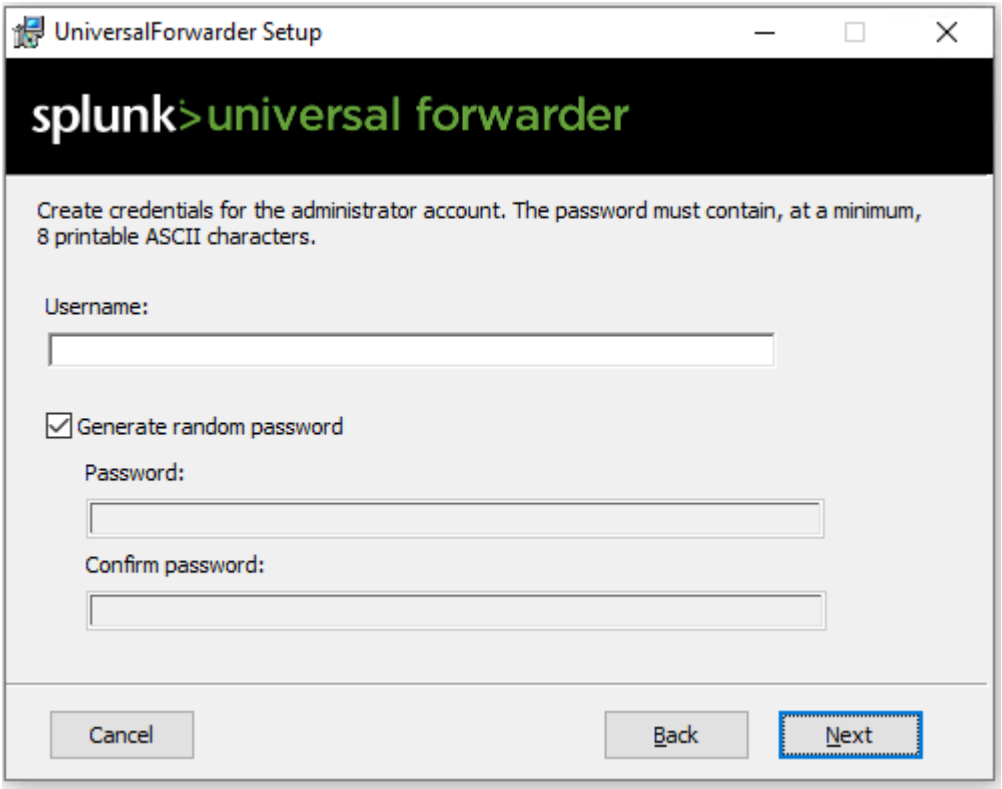
2. Seleccionamos en nuestro caso la versión 9.4.0 de Splunk para Windows 64-bit.



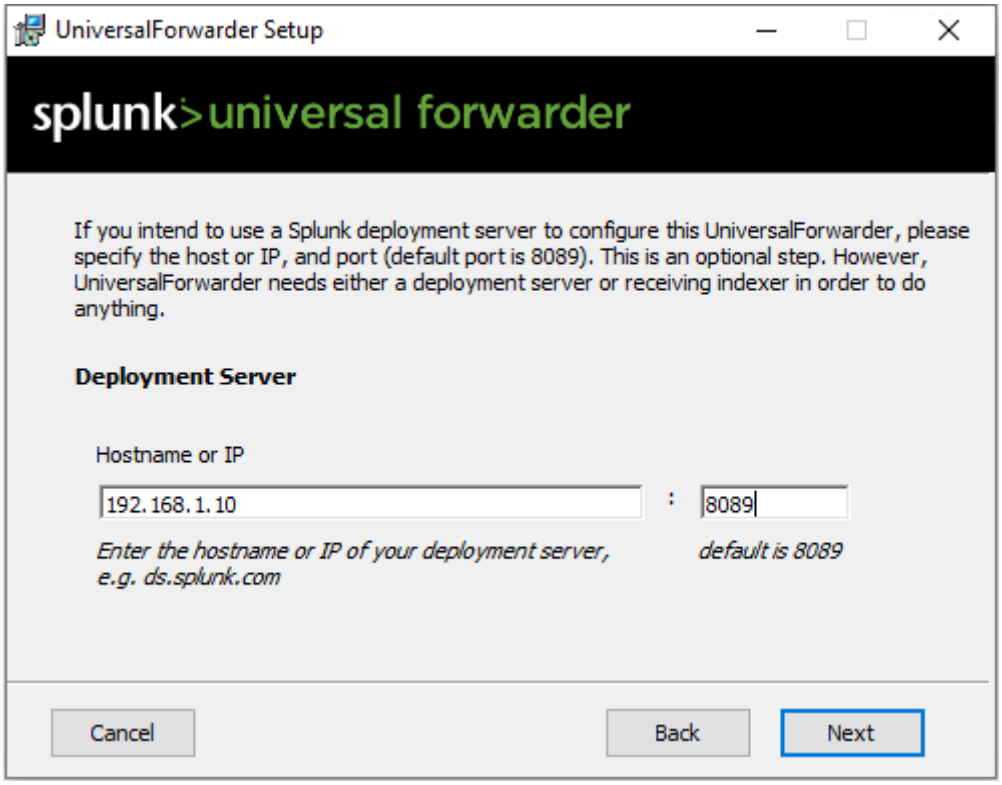
3. Ejecutar el instalador de la versión 9.4.0 de Splunk, aceptar licencia y continuar.



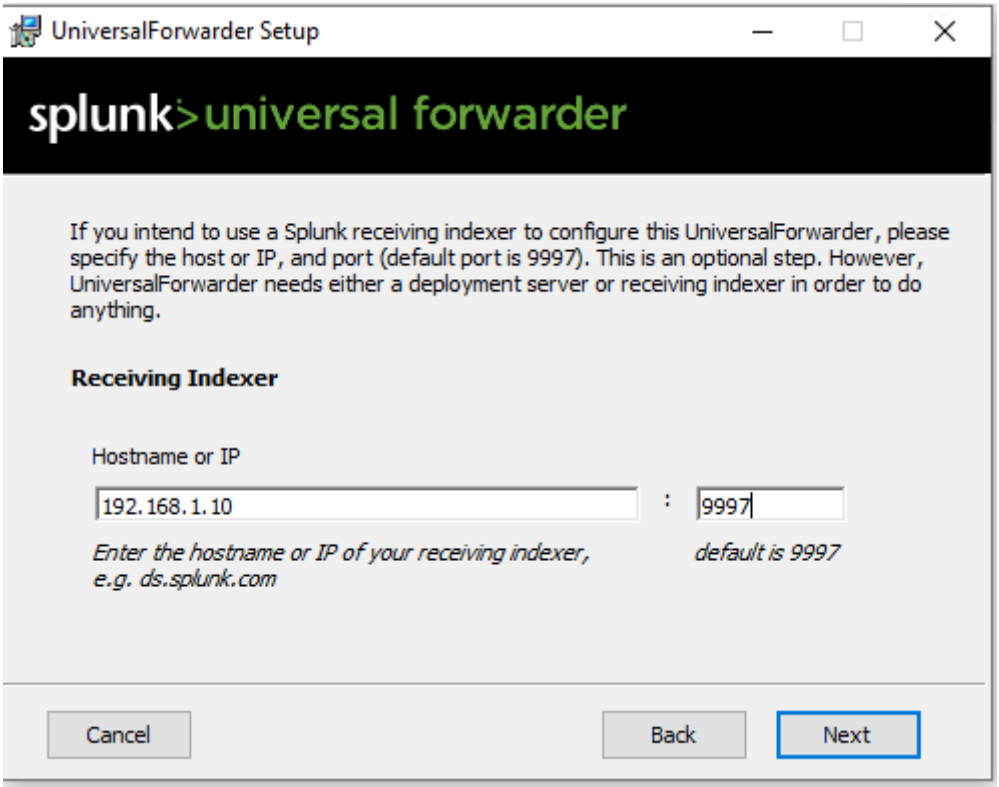
4. Crear una cuenta de administrador local.



5. Ingresar la dirección IP de la instancia de Splunk que está en ejecución en el servidor Ubuntu con el puerto por defecto.

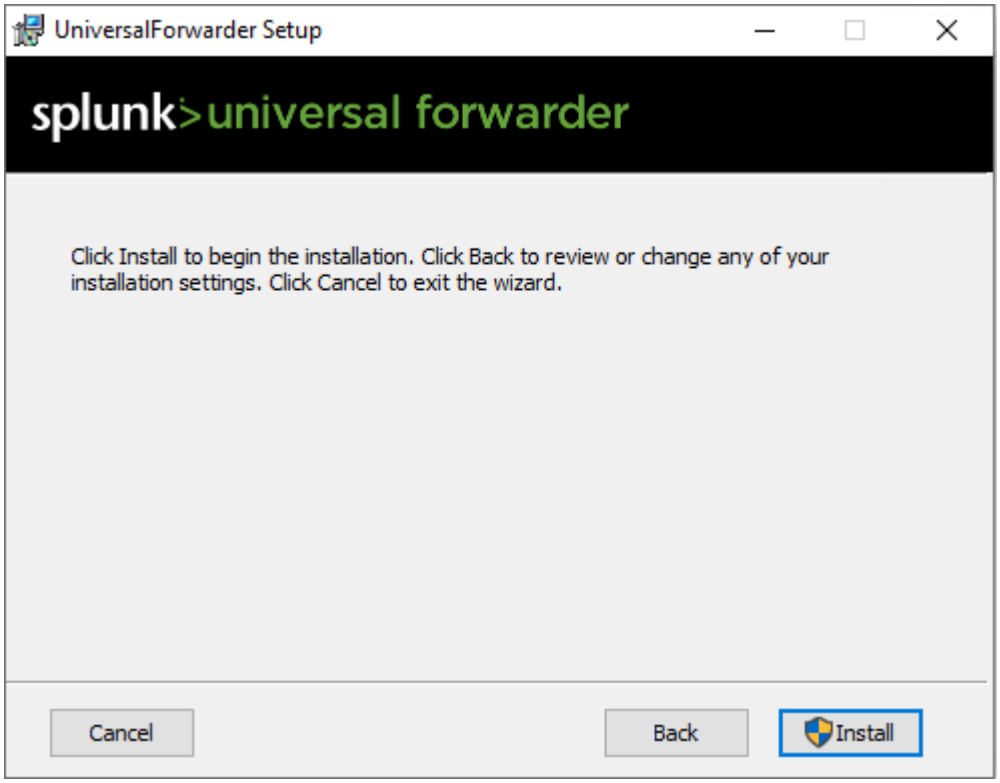


6. Ingresar la dirección IP de la instancia de Splunk que está en ejecución en el servidor Ubuntu con el puerto por defecto.

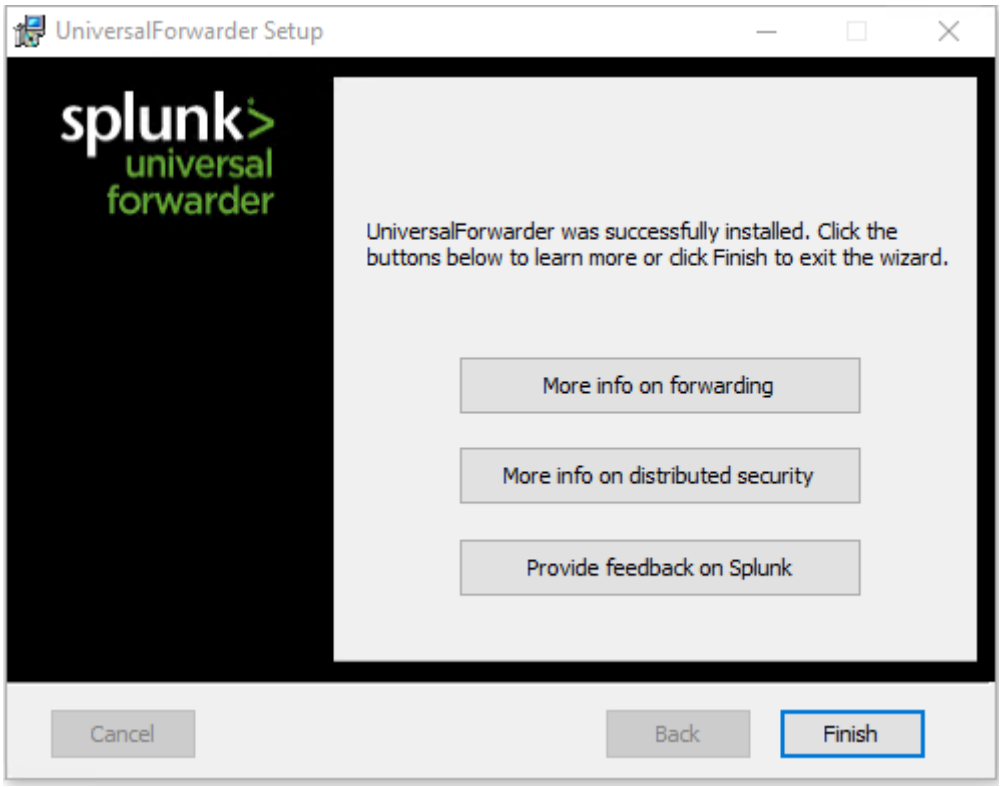


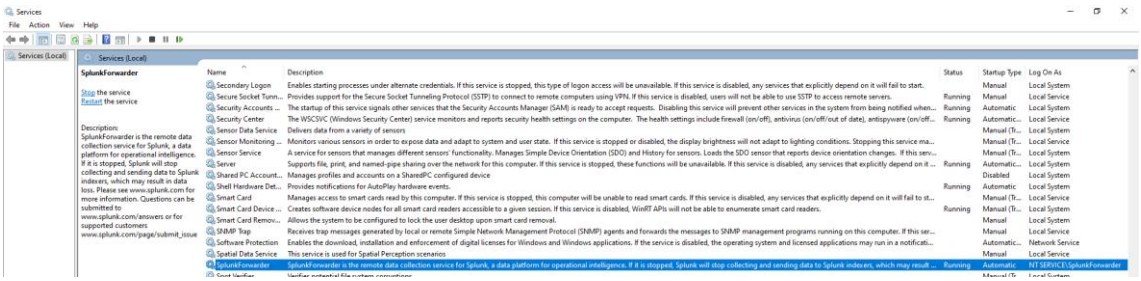
A

7. Instalar



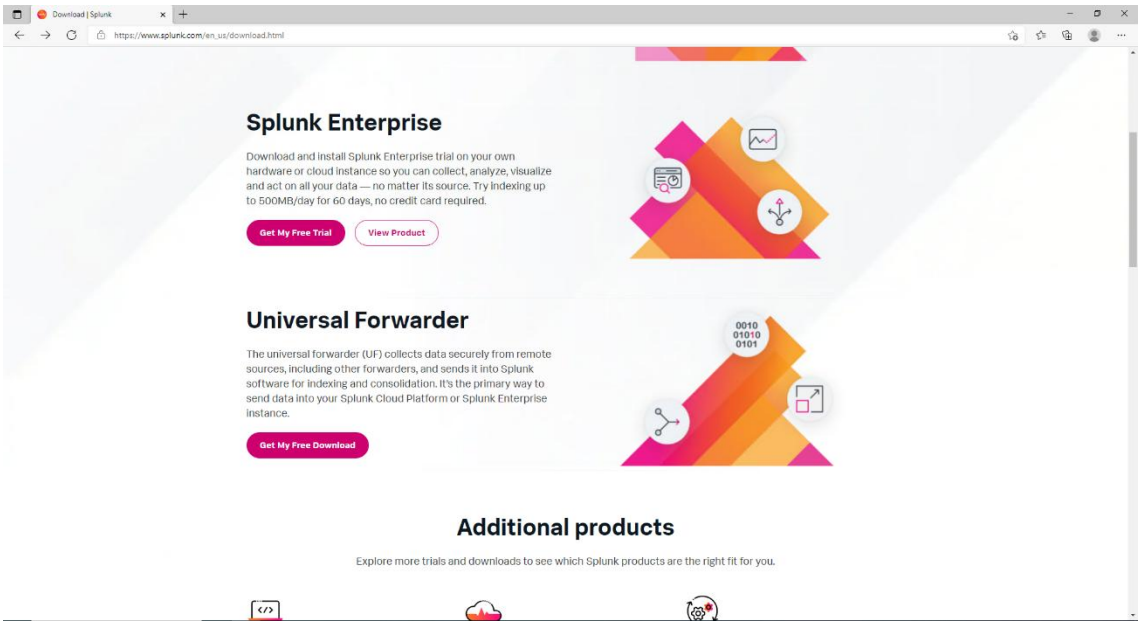
8. Verificar que el servicio está corriendo en el host.



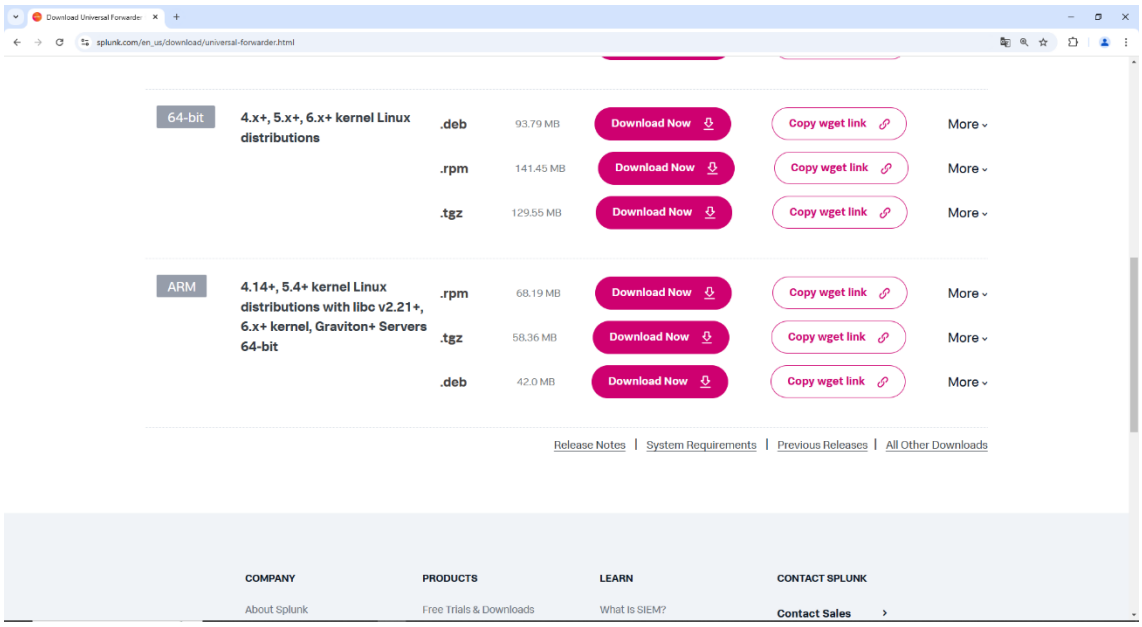


Instalación de UF en Ubuntu

1. Para instalar el Universal Forwarder utilizaremos la documentación oficial de Splunk [12] Descargar el instalador del Universal Forwarder desde la página oficial de Splunk



1. Seleccionamos en nuestro caso Linux 64-bit .deb



2. Copiar el instalador en el /tmp del servidor Ubuntu

```
root@franciscoubuntuserver:~# cd /tmp/
root@franciscoubuntuserver:/tmp# ls
snap-private-tmp
splunkforwarder-9.4.0-6b4ebe426ca6-linux-amd64.deb
systemd-private-fc0076cb38044200bf8728aef52ea293-ModemManager.service-HXHQQW
systemd-private-fc0076cb38044200bf8728aef52ea293-systemd-logind.service-StRNdM
systemd-private-fc0076cb38044200bf8728aef52ea293-systemd-resolved.service-CIvzC8
systemd-private-fc0076cb38044200bf8728aef52ea293-systemd-timesyncd.service-bPALYO
root@franciscoubuntuserver:/tmp# _
```

3. Ejecutar el siguiente comando para la instalación:

   Sudo splunkforwarder-9.4.0-6b4ebe426ca6-linux-amd64.deb

```
root@franciscoubuntuserver:/opt/splunkforwarder/bin# cd /tmp/
root@franciscoubuntuserver:/tmp# ls
snap-private-tmp
splunkforwarder-9.4.0-6b4ebe426ca6-linux-amd64.deb
systemd-private-fc0076cb38044200bf8728aef52ea293-ModemManager.service-HXHQQW
systemd-private-fc0076cb38044200bf8728aef52ea293-systemd-logind.service-StRNdM
systemd-private-fc0076cb38044200bf8728aef52ea293-systemd-resolved.service-CIvzC8
systemd-private-fc0076cb38044200bf8728aef52ea293-systemd-timesyncd.service-bPALYO
root@franciscoubuntuserver:/tmp# dpkg -i splunkforwarder-9.4.0-6b4ebe426ca6-linux-amd64.deb _
```

4. Para que Splunk se ejecute automáticamente después de que se inicie el servidor es necesario ejecutar el siguiente comando [10]:

   sudo opt/splunk/bin/./splunk enable boot-start

```
root@franciscoubuntuserver:/opt/splunkforwarder/bin# cd /tmp/
root@franciscoubuntuserver:/tmp# ls
snap-private-tmp
splunkforwarder-9.4.0-6b4ebe426ca6-linux-amd64.deb
systemd-private-fc0076cb38044200bf8728aef52ea293-ModemManager.service-HXHQQW
systemd-private-fc0076cb38044200bf8728aef52ea293-systemd-logind.service-StRNdM
systemd-private-fc0076cb38044200bf8728aef52ea293-systemd-resolved.service-CIvzC8
systemd-private-fc0076cb38044200bf8728aef52ea293-systemd-timesyncd.service-bPALYO
root@franciscoubuntuserver:/tmp# dpkg -i splunkforwarder-9.4.0-6b4ebe426ca6-linux-amd64.deb
dpkg: warning: files list file for package 'splunkforwarder' missing; assuming package has no files
currently installed
(Reading database ... 73776 files and directories currently installed.)
Preparing to unpack splunkforwarder-9.4.0-6b4ebe426ca6-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunkforwarder (9.4.0) over (9.4.0) ...
Setting up splunkforwarder (9.4.0) ...
find: ‘/opt/splunkforwarder/lib/python3.7/site-packages’: No such file or directory
find: ‘/opt/splunkforwarder/lib/python3.9/site-packages’: No such file or directory
complete
root@franciscoubuntuserver:/tmp# cd /opt/splunkforwarder/bin/
root@franciscoubuntuserver:/opt/splunkforwarder/bin# ./splunk enable boot-start
```

Aceptar la licencia y crear usuario y password para administrar Splunk

```
Third Party Providers: Your authorized consultants, contractors, and agents.

Trial Offering: An Offering we make available on a trial or evaluation basis.

Usage Data: Data generated from the usage, configuration, deployment, access,
and performance of an Offering.

Use Rights: As set out in section 1.1.

Do you agree with this license? [y/n]: y

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: splunk
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
ERROR: Password did not meet complexity requirements. Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
ERROR: Password did not meet complexity requirements. Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Creating unit file...
The unit file has been created.

Important: splunk will start under systemd as user: splunkfwd
Systemd unit file installed by user at /etc/systemd/system/SplunkForwarder.service.
Configured as systemd managed service.
root@franciscoubuntuserver:/opt/splunkforwarder/bin#
```

Verifico si el servicio está corriendo con el siguiente comando:

sudo ./splunk status

Si no está en funcionamiento, ejecutar el siguiente comando:

sudo opt/splunk/bin/./splunk start

```
root@franciscoubuntuserver:/opt/splunkforwarder/bin# ./splunk start
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"

Splunk> See your world.  Maybe wish you hadn't.

Checking prerequisites...
        Checking mgmt port [8089]: open
                Creating: /opt/splunkforwarder/var/lib/splunk
                Creating: /opt/splunkforwarder/var/run/splunk
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/i18n
                Creating: /opt/splunkforwarder/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunkforwarder/var/run/splunk/upload
                Creating: /opt/splunkforwarder/var/run/splunk/search_telemetry
                Creating: /opt/splunkforwarder/var/run/splunk/search_log
                Creating: /opt/splunkforwarder/var/spool/splunk
                Creating: /opt/splunkforwarder/var/spool/dirmoncache
                Creating: /opt/splunkforwarder/var/lib/splunk/authDb
                Creating: /opt/splunkforwarder/var/lib/splunk/hashDb
                Creating: /opt/splunkforwarder/var/run/splunk/collect
                Creating: /opt/splunkforwarder/var/run/splunk/sessions
New certs have been generated in '/opt/splunkforwarder/etc/auth'.
        Checking conf files for problems...
        Done
        Checking default conf files for edits...
        Validating installed files against hashes from '/opt/splunkforwarder/splunkforwarder-9.4.0-6
b4ebe426ca6-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

root@franciscoubuntuserver:/opt/splunkforwarder/bin#
```

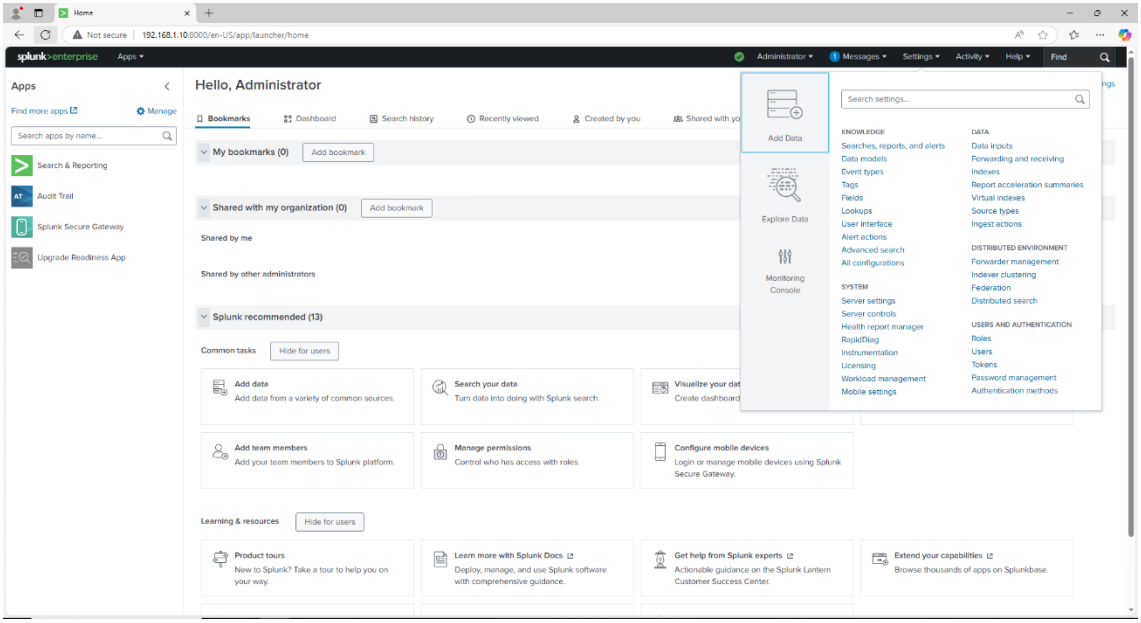
5. Agregamos la dirección del Indexer para reenviar los logs utilizando el siguiente comando:

   ./splunk add forward-server 192.168.1.10:9997

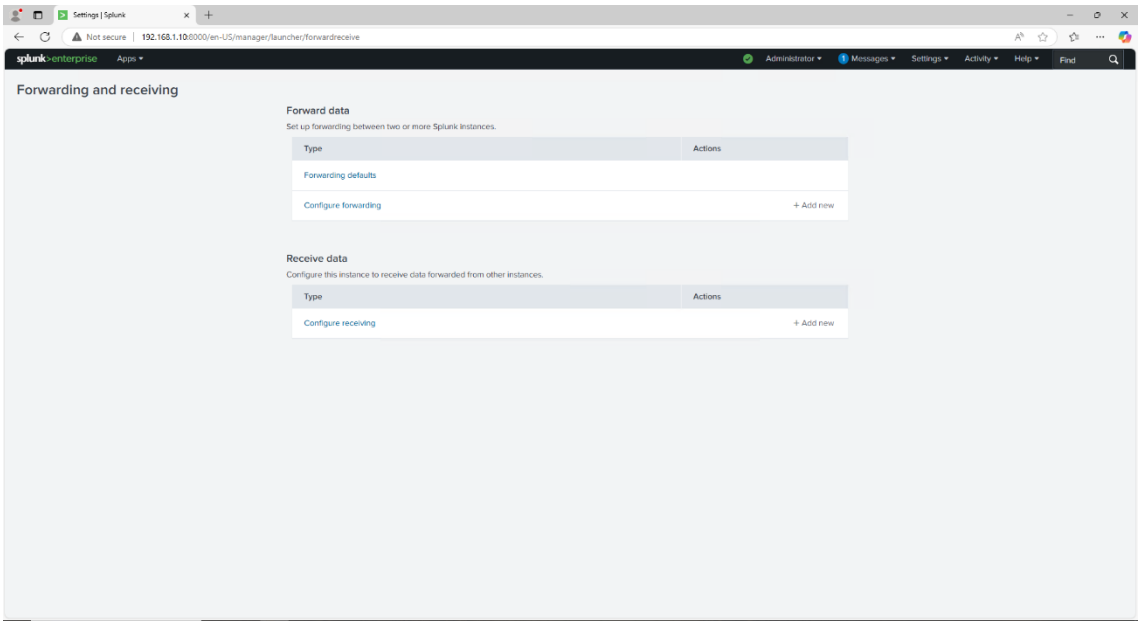
```
root@franciscoubuntuserver:/opt/splunkforwarder/bin# ./splunk add forward-server 192.168.1.10:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Splunk username: splunk
Password:
Added forwarding to: 192.168.1.10:9997.
root@franciscoubuntuserver:/opt/splunkforwarder/bin#
```

Habilitar receptor para escuchar en el puerto tcp 9997

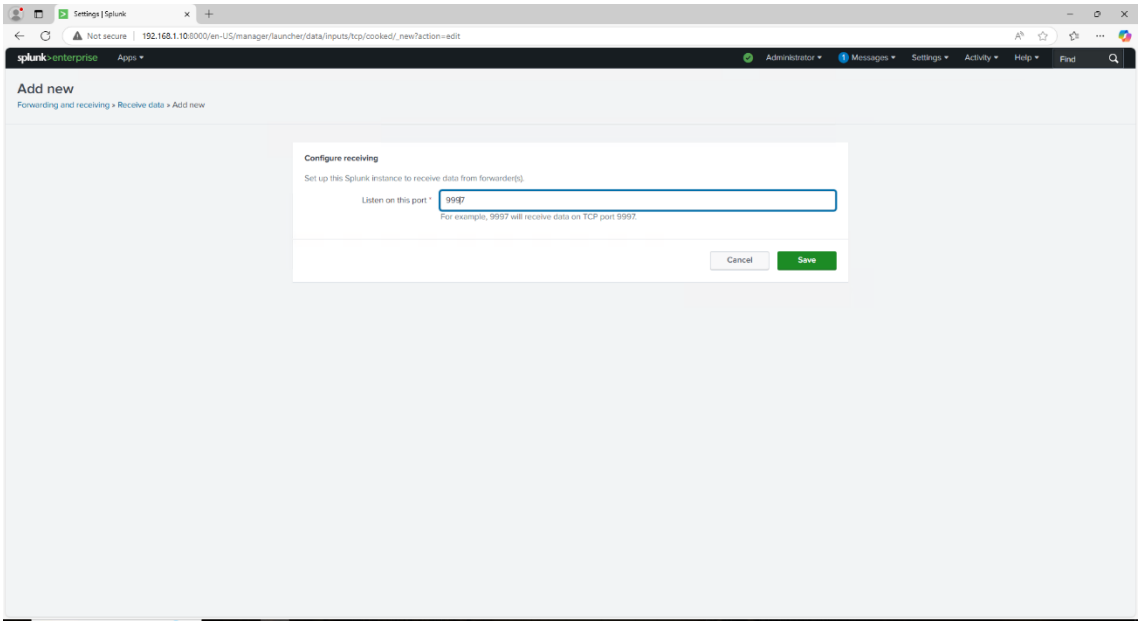
1. Seleccionamos “Settings” > “Add Data” > “Forwarding and receiving”



2. Seleccionamos “Receive data” > “+Add new”

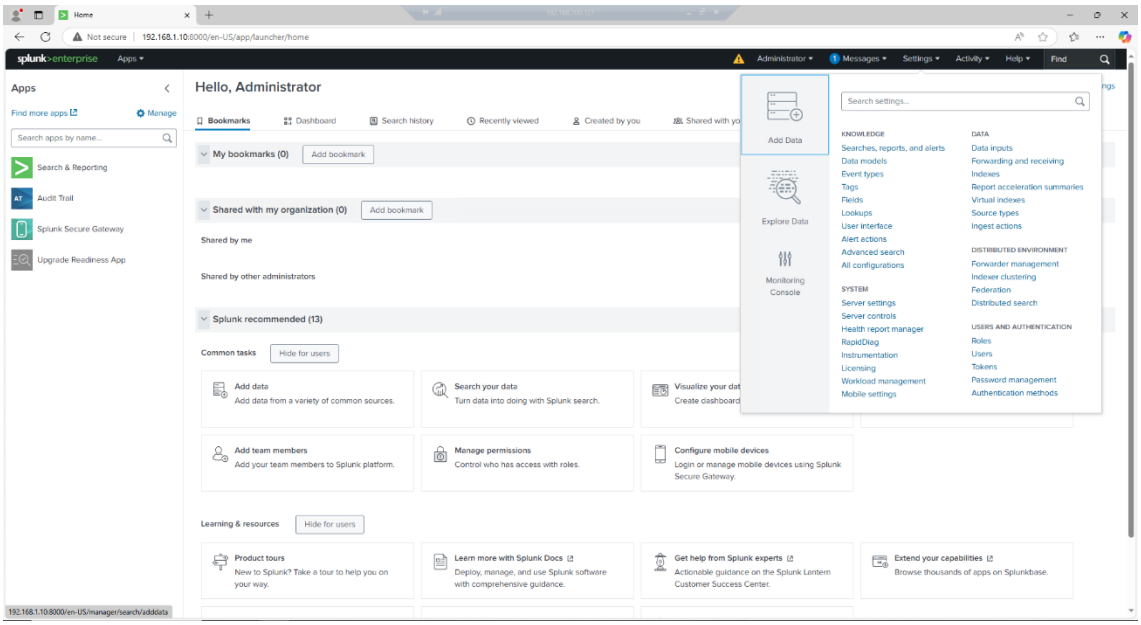


3. Ingresamos el puerto 9997 que es el puerto predeterminado, y el mismo que se configuró en los Universal Forwarders

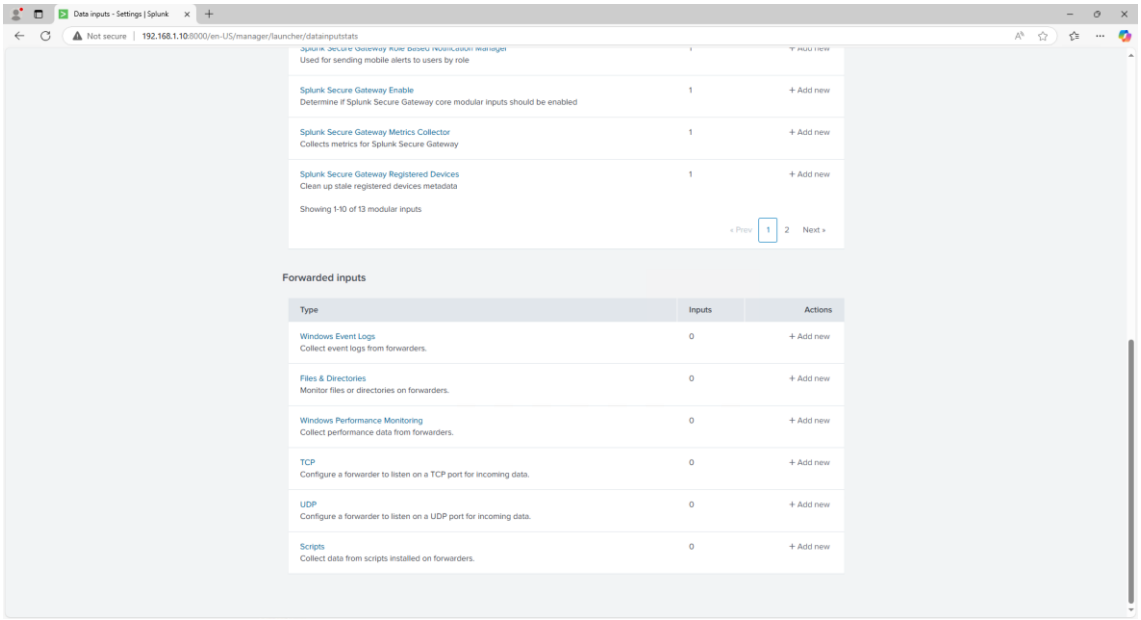


Configurar recepción de datos desde UFs en Windows

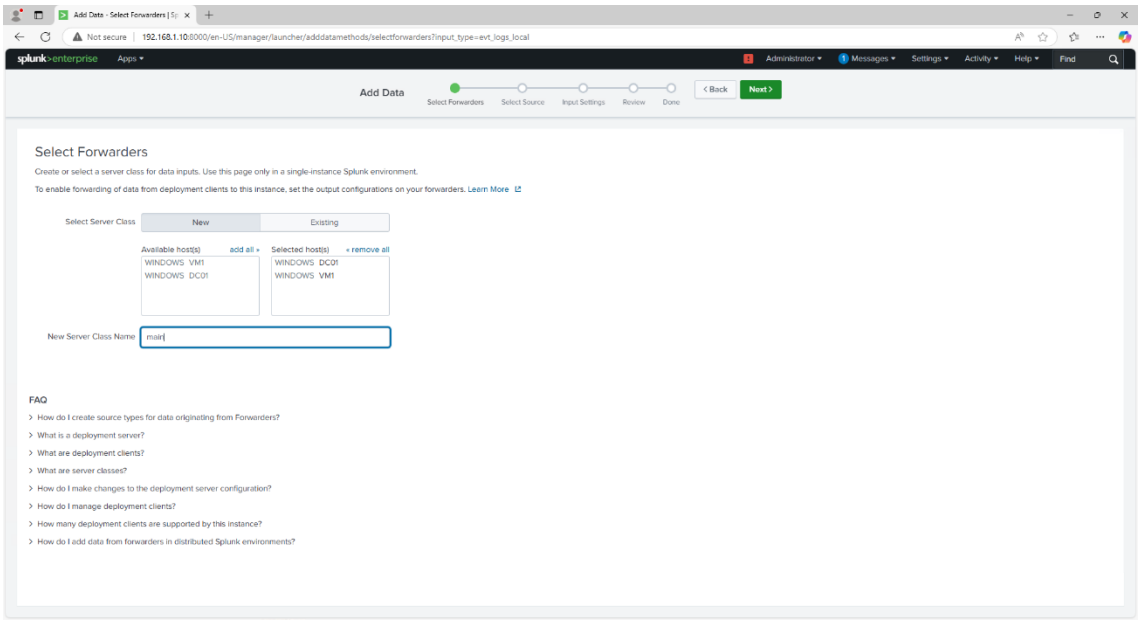
1. Seleccionamos “Settings” > “DATA” > “Data Inputs”



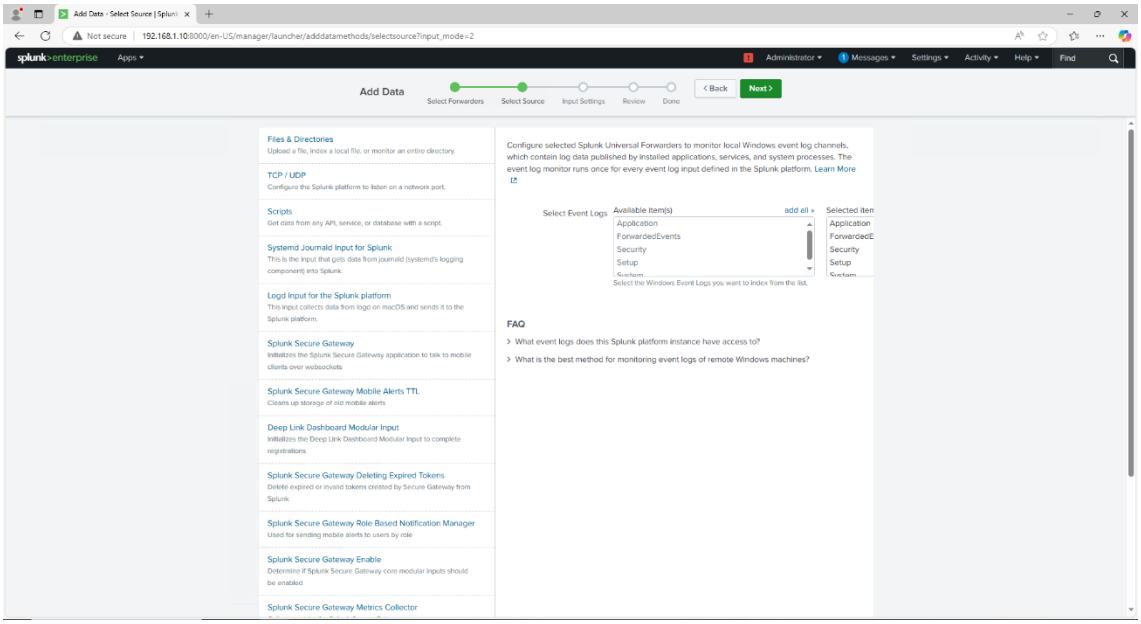
2. Seleccionamos “Forwarded input” > “Windows Event logs” > “+Add new”



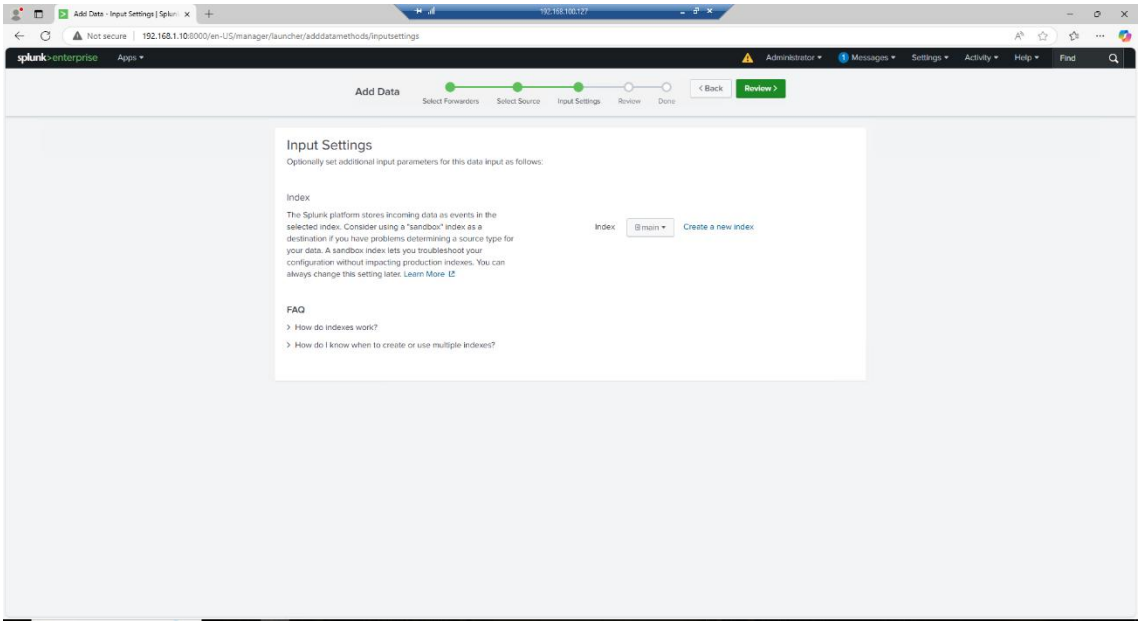
3. En esta página podemos ver los UFs que están disponibles y configurados para ser incorporados. Los agregamos seleccionando “add all”, creamos una nueva server class “main” y seleccionamos “next”



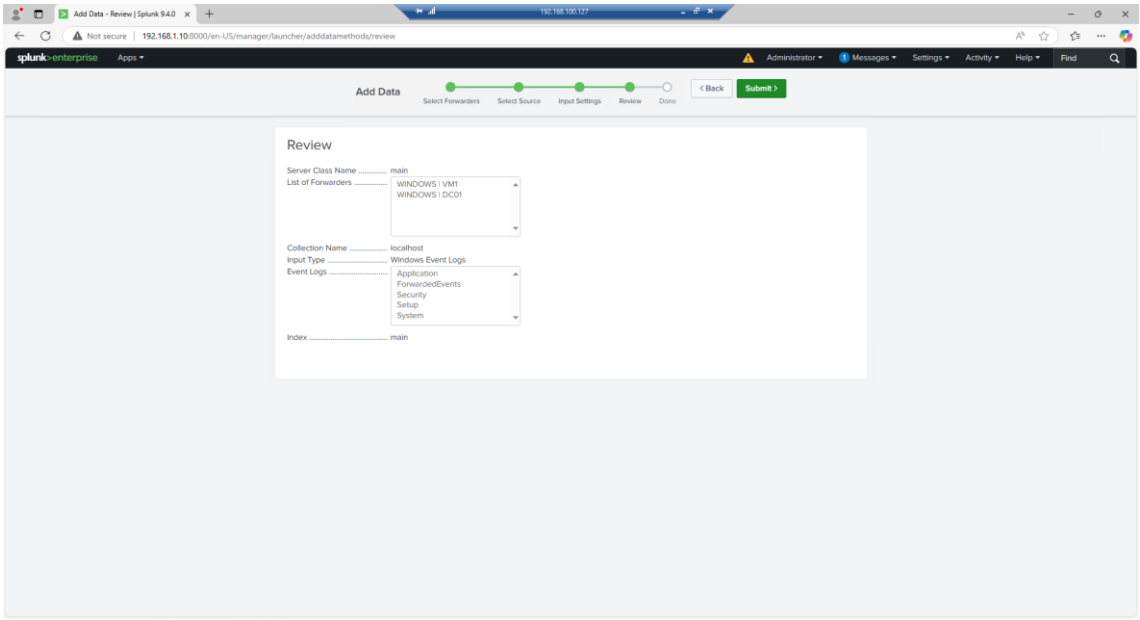
4. Incorporamos todos los eventos de Windows seleccionando “add all”



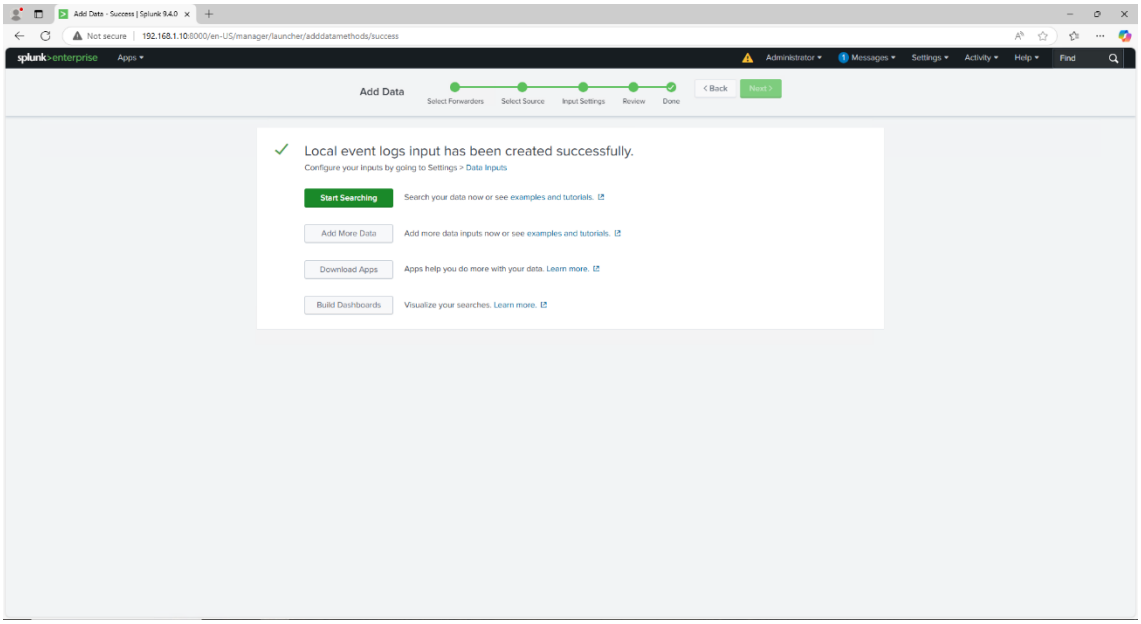
5. Seleccionamos el index “main”



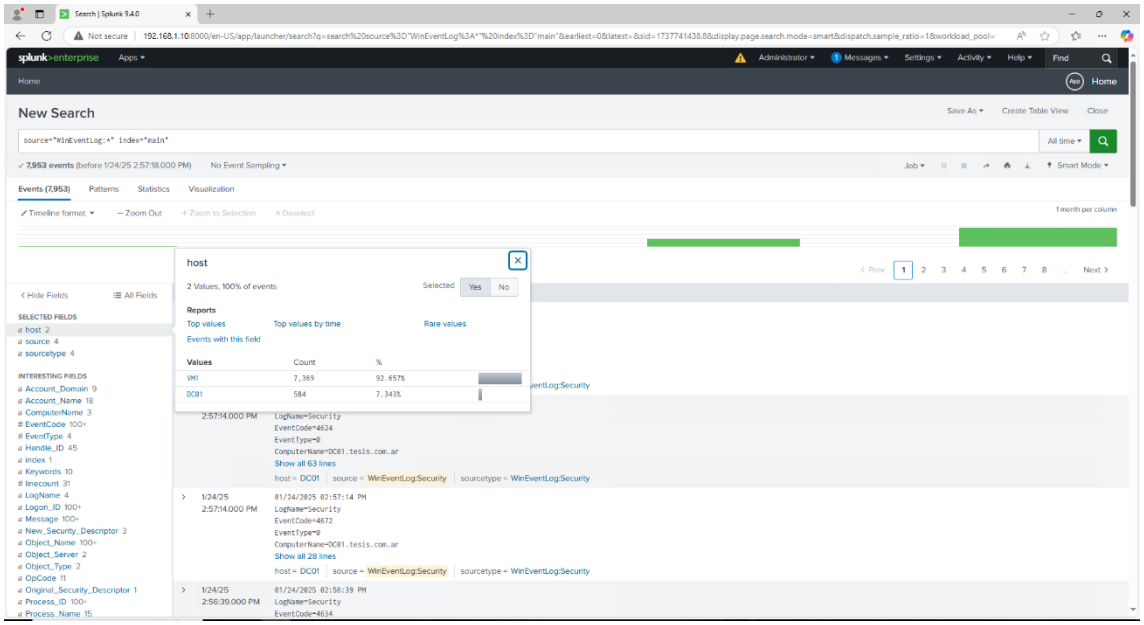
6. Revisamos lo configurado.



7. Ingresamos a “Start Searching” para confirmar que ya se estén recibiendo eventos.

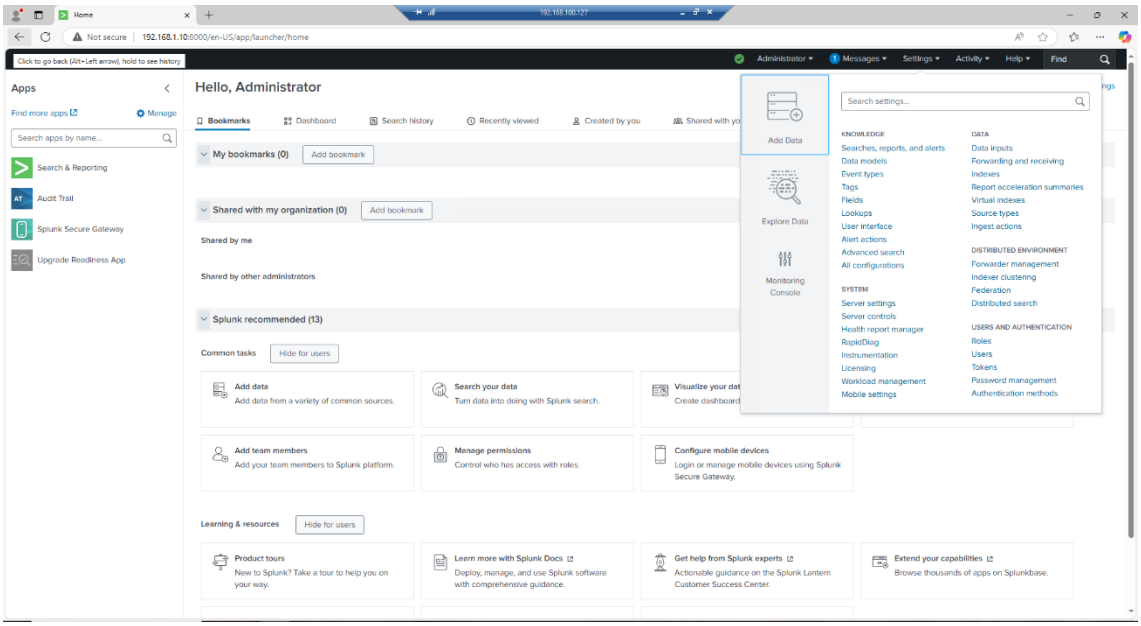


8. Verificamos que ya estamos visualizando eventos correspondientes a los 2 host que poseen un UF instalado.

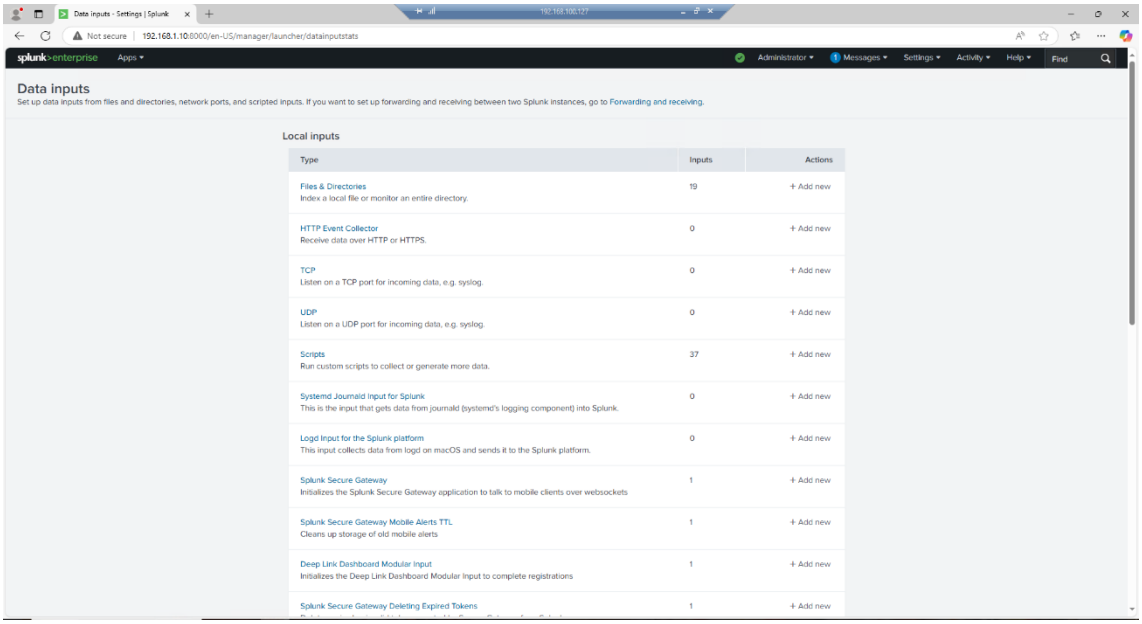


Configurar recepción de datos desde reenvíos por syslog

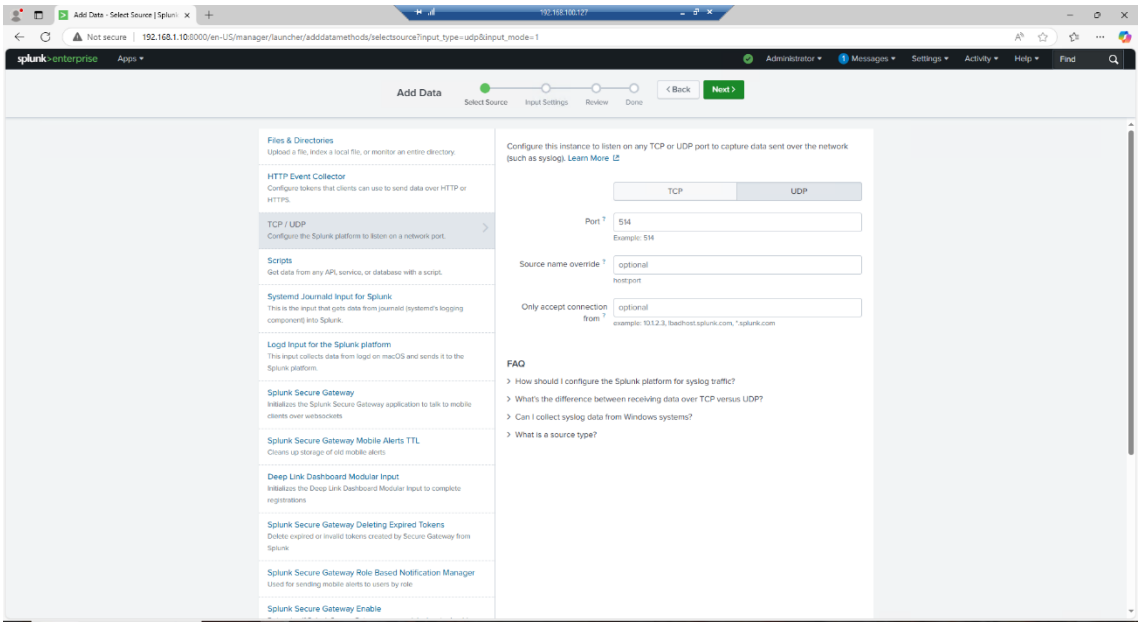
1. Seleccionamos “Settings” > “Add Data” > “Data Inputs”



2. Seleccionamos “UDP”

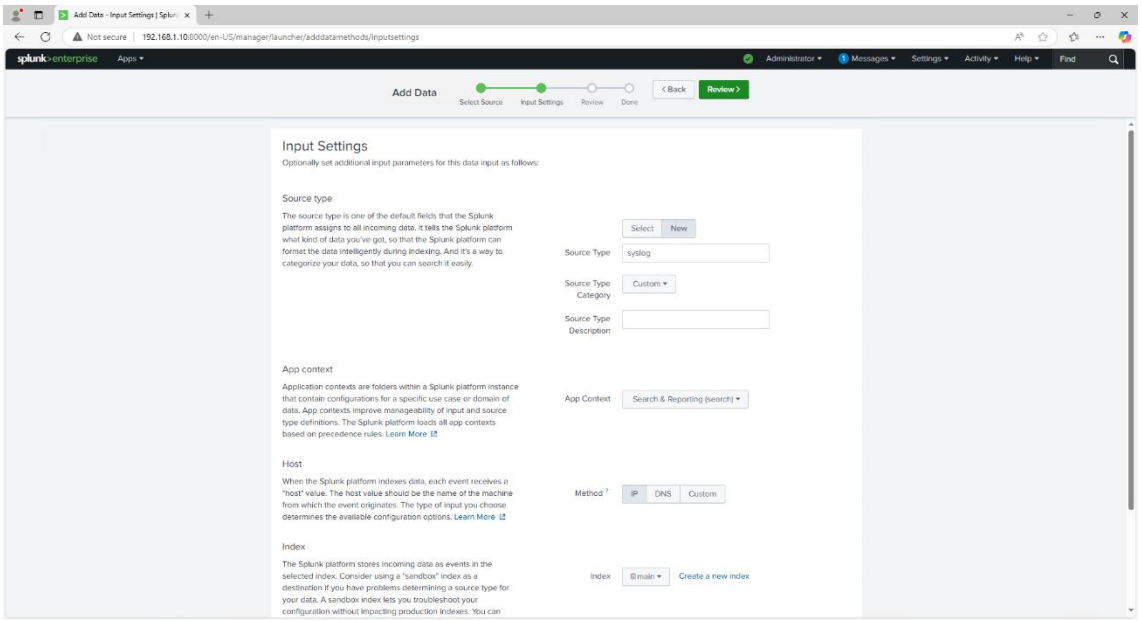


3. Ingresamos en Port “514”

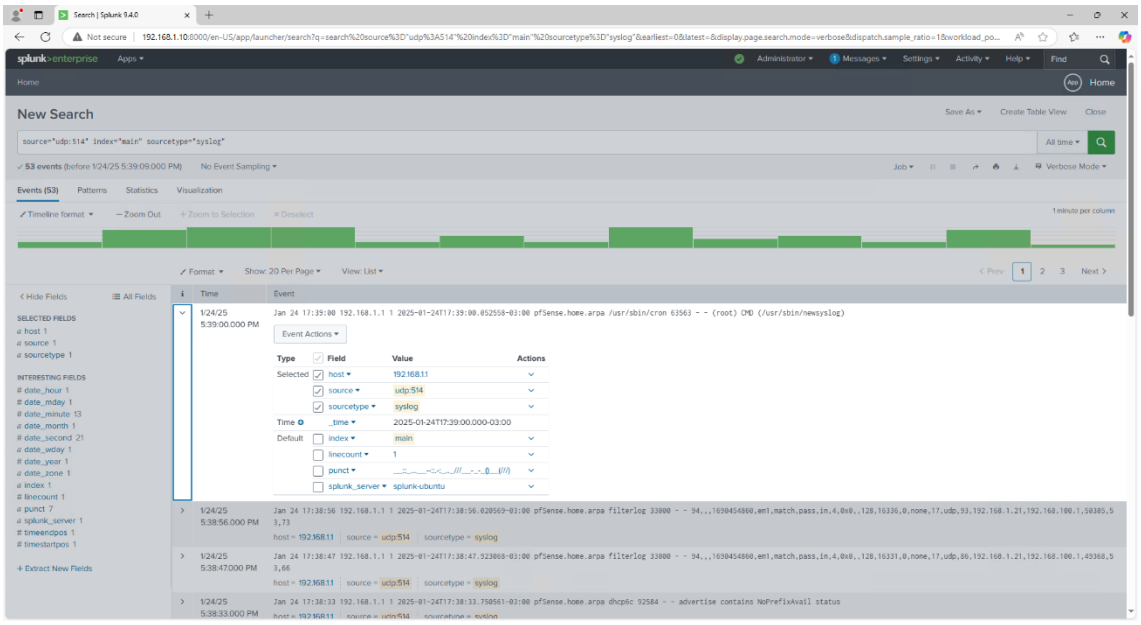


4. Seleccionamos “New”

   Ingresamos en sourcetype:”syslog” y en app context:”search and reporting”

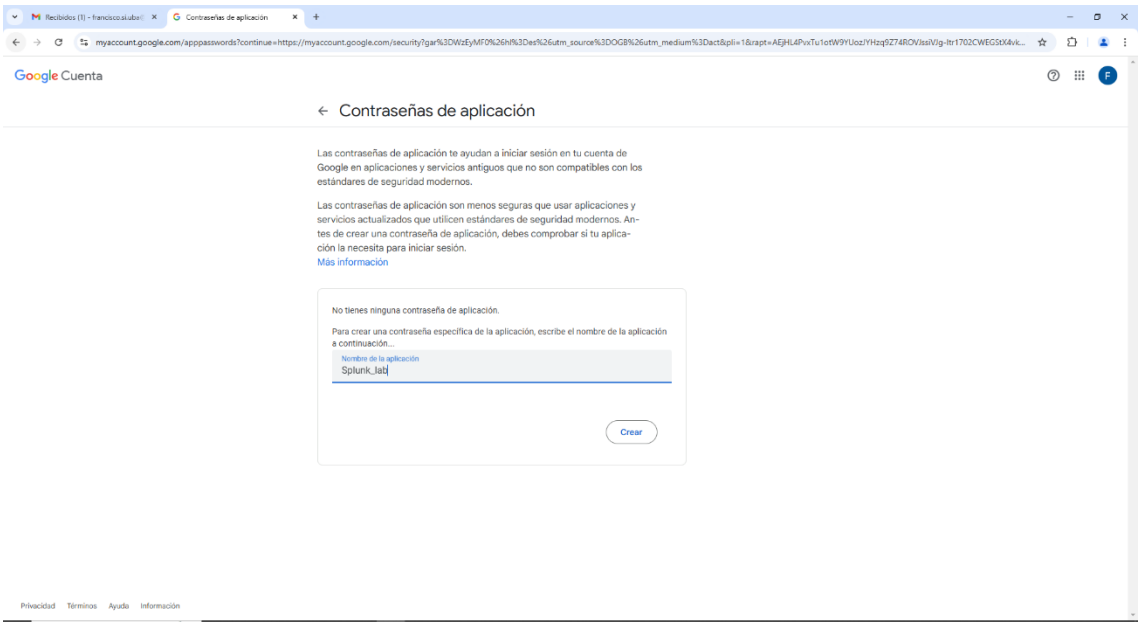


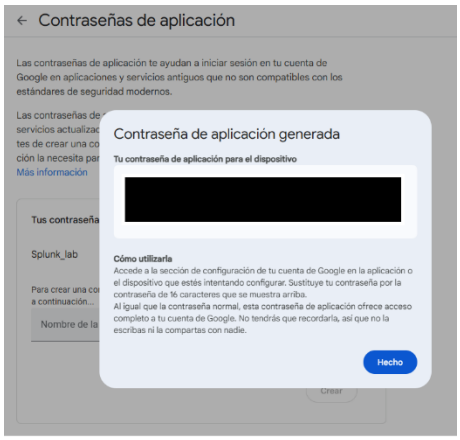
5. Finalizamos y verificamos la recepción de los eventos.



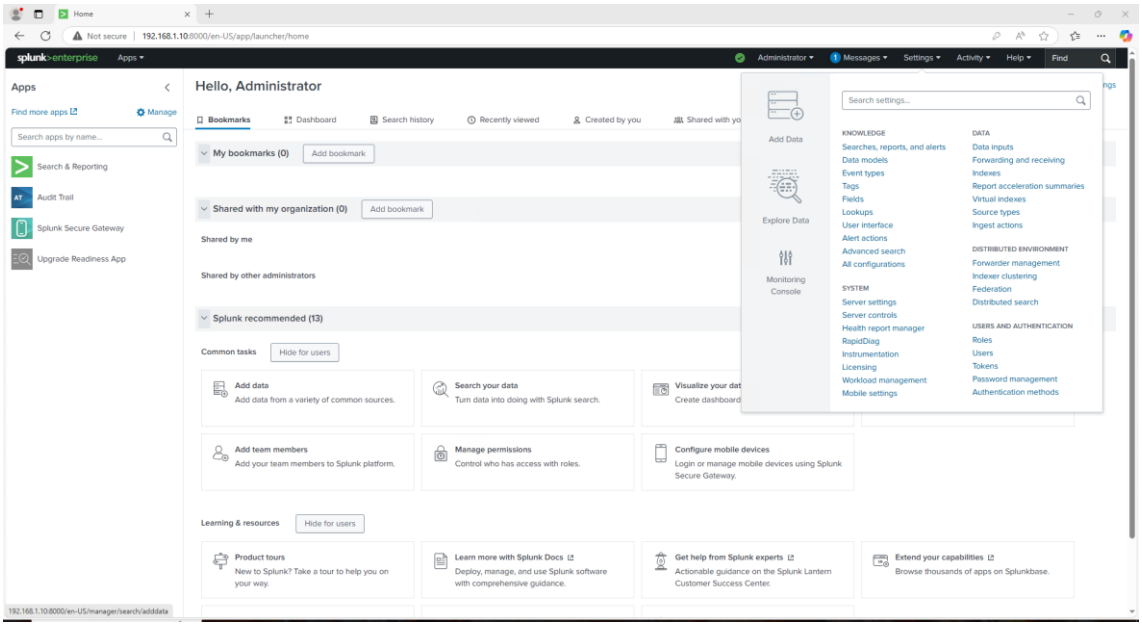
Configuración de SMTP en Splunk

1. Creamos una contraseña de aplicación en la cuenta francisco.si.uba@gmail.com que será utilizada por Splunk para poder enviar correos a través de esta cuenta.

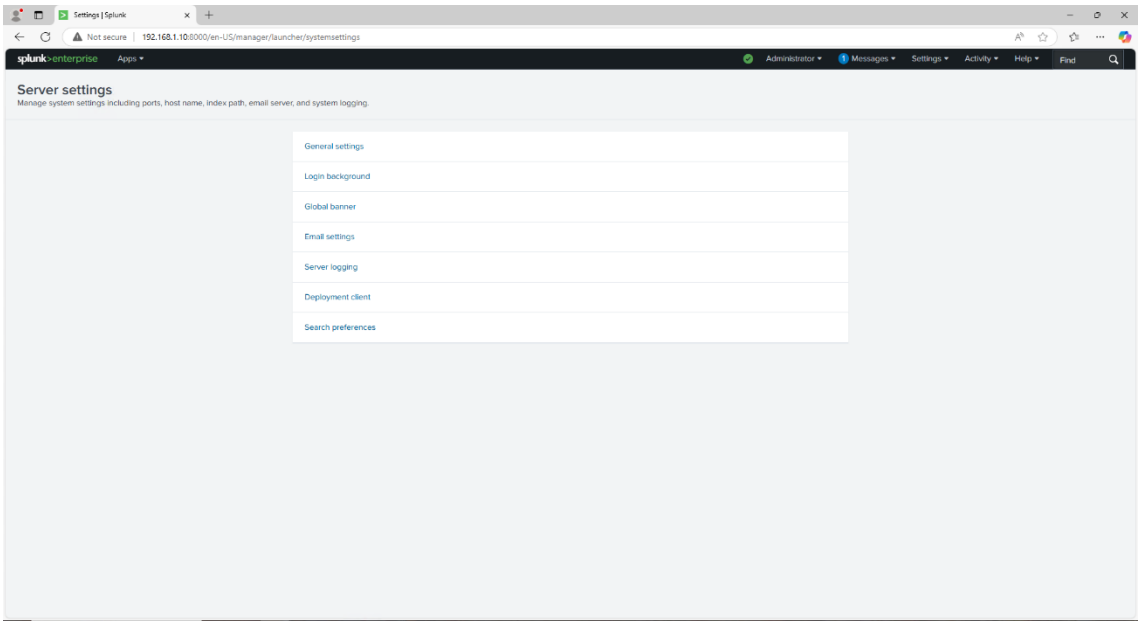




2. Seleccionamos “Settings” > “SYSTEM” > “Server Settings”



3. Seleccionamos “Email settings”



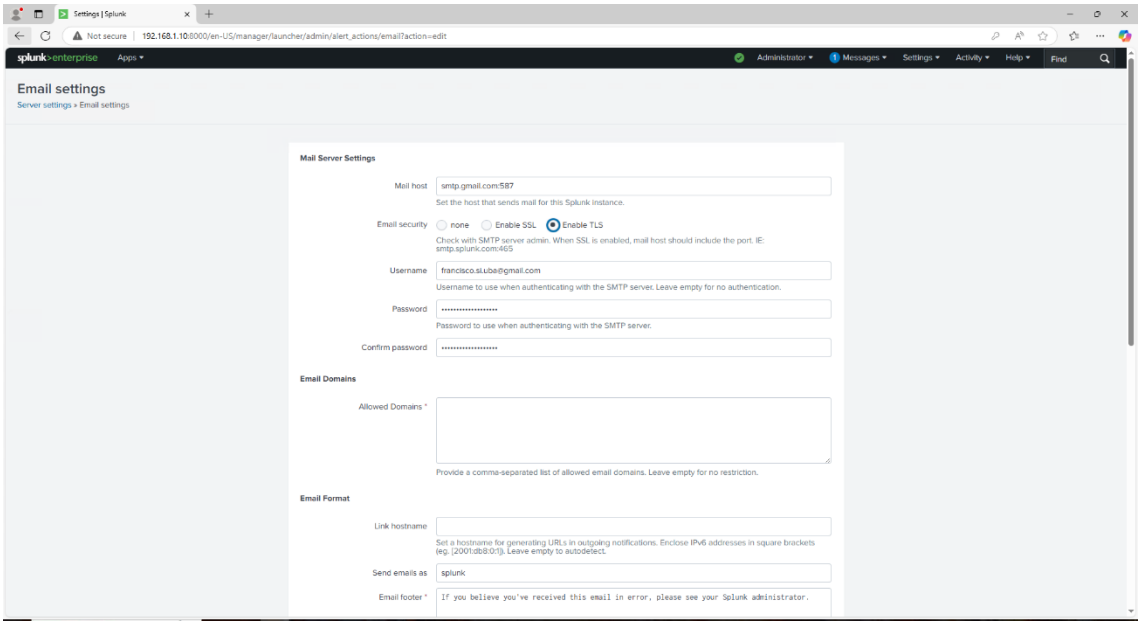
4. Ingresamos en:

   Mail host: “smtp.gmail.com:587”

   Email security:”Enable TLS”

   Username:francisco.si.uba@gmail.com

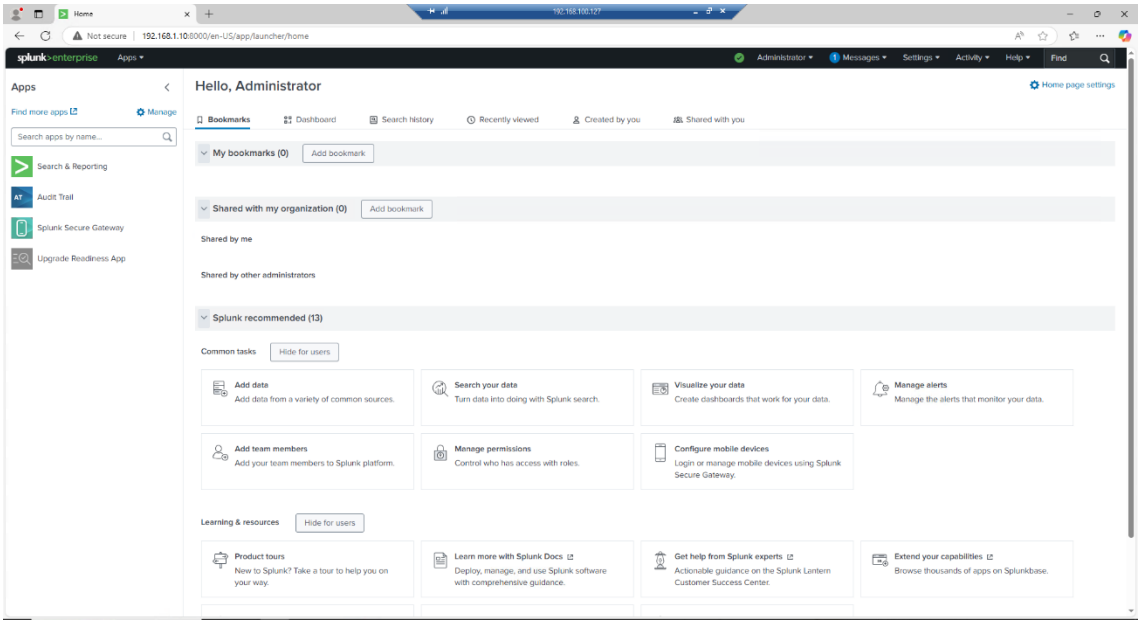
   Password: la contraseña de aplicación generada



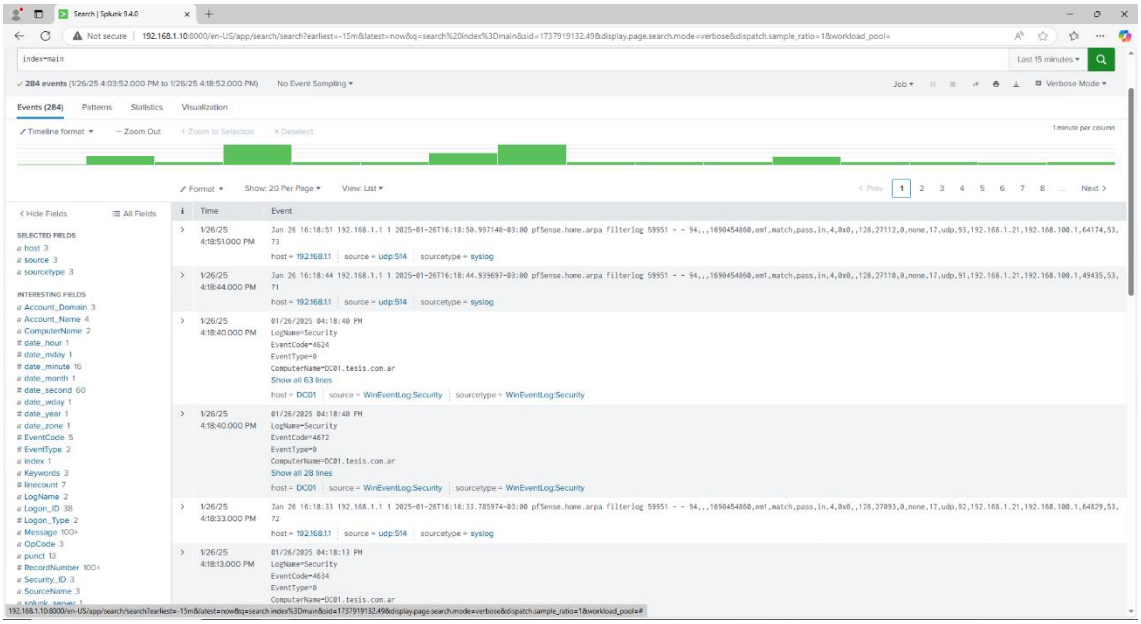
Configuración caso de uso referido a Windows

A continuación, se presenta como ejemplo el siguiente caso de uso: Detección de múltiples intentos de inicio de sesión fallidos en un host en un corto período de tiempo.

1. Ingresamos la App de “Seach & Reporting”

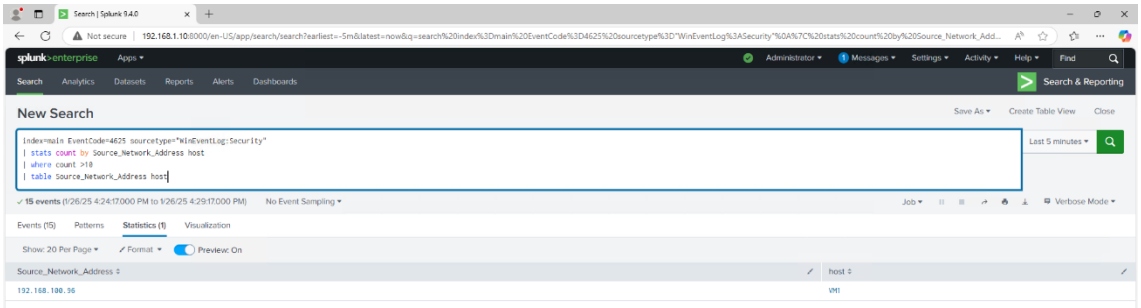


2. En el buscador “Search” realizamos una primera búsqueda especificando el índice que contiene la información de los eventos que buscamos.
   En este caso utilizamos index=main y filtramos los últimos 15 minutos.

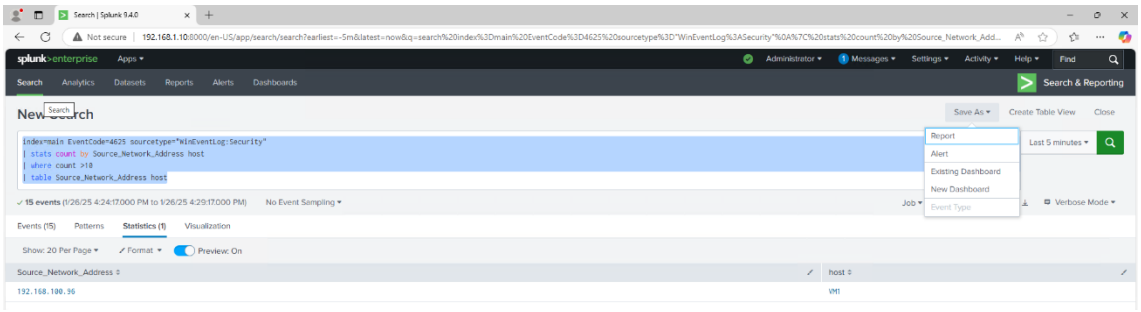


En nuestro caso queremos crear un caso de uso que se active cuando en un host Windows con un Universal Forwarder, que este reportando a Splunk, registre más de 10 intentos fallidos de inicio de sesion en menos de 5 min. Estas mismas condiciones se pueden presentar como la siguiente búsqueda en Splunk:

index=main EventCode=4625 sourcetype="WinEventLog:Security"
| stats count by Source_Network_Address host
| where count >10
| table Source_Network_Address host



3. Una vez que la búsqueda refleja correctamente el objetivo de nuestro caso de uso, la guardamos como una alerta seleccionando “Save As”>”Alert”

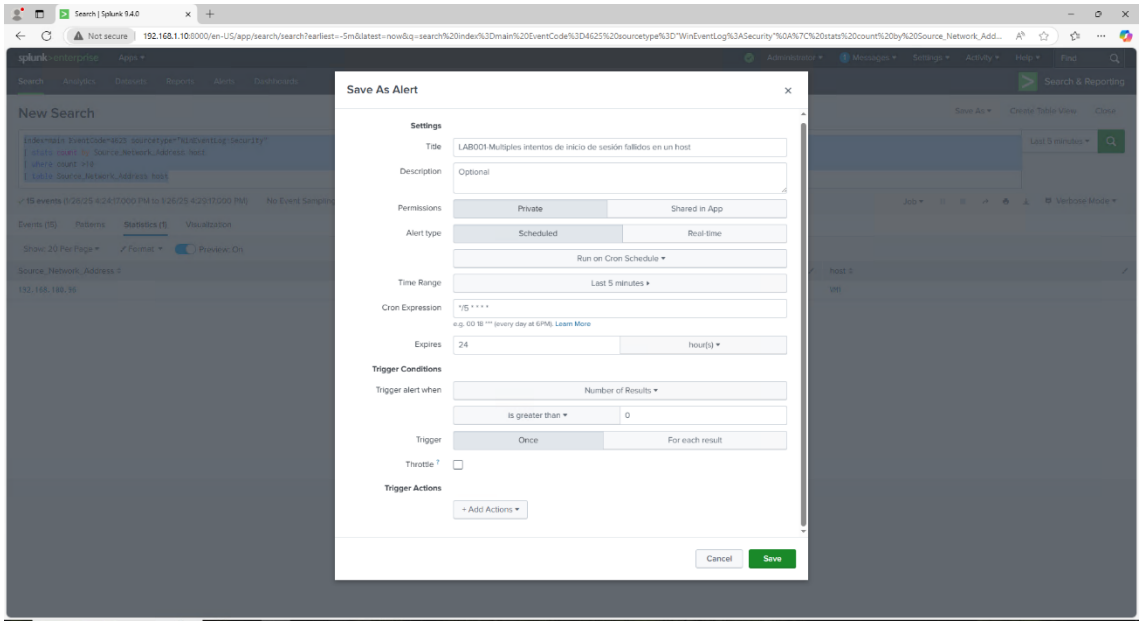


4. Ingresamos los siguientes datos:

   Title: “LAB001-Multiples intentos de inicio de sesión fallidos en un host”

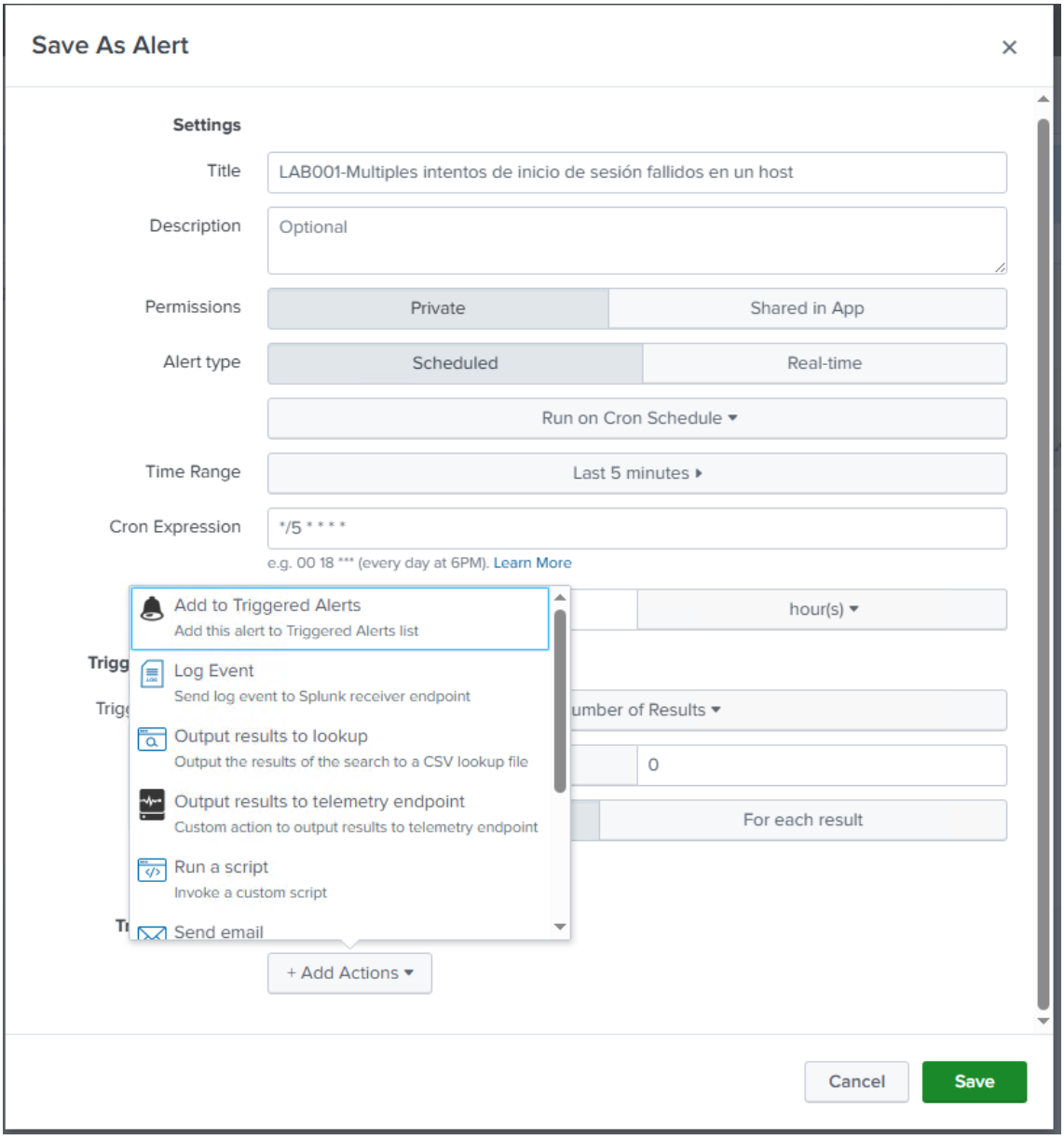
   Alert type: “Scheduled”, "Run on Cron Schedule” (esta opción es para configurar una búsqueda periódica)

   Cron Expresssion: */5 * * * * (indica que la tarea se ejecutará cada 5 minutos, a cualquier hora, todos los días del mes, durante todos los meses y todos los días de la semana)

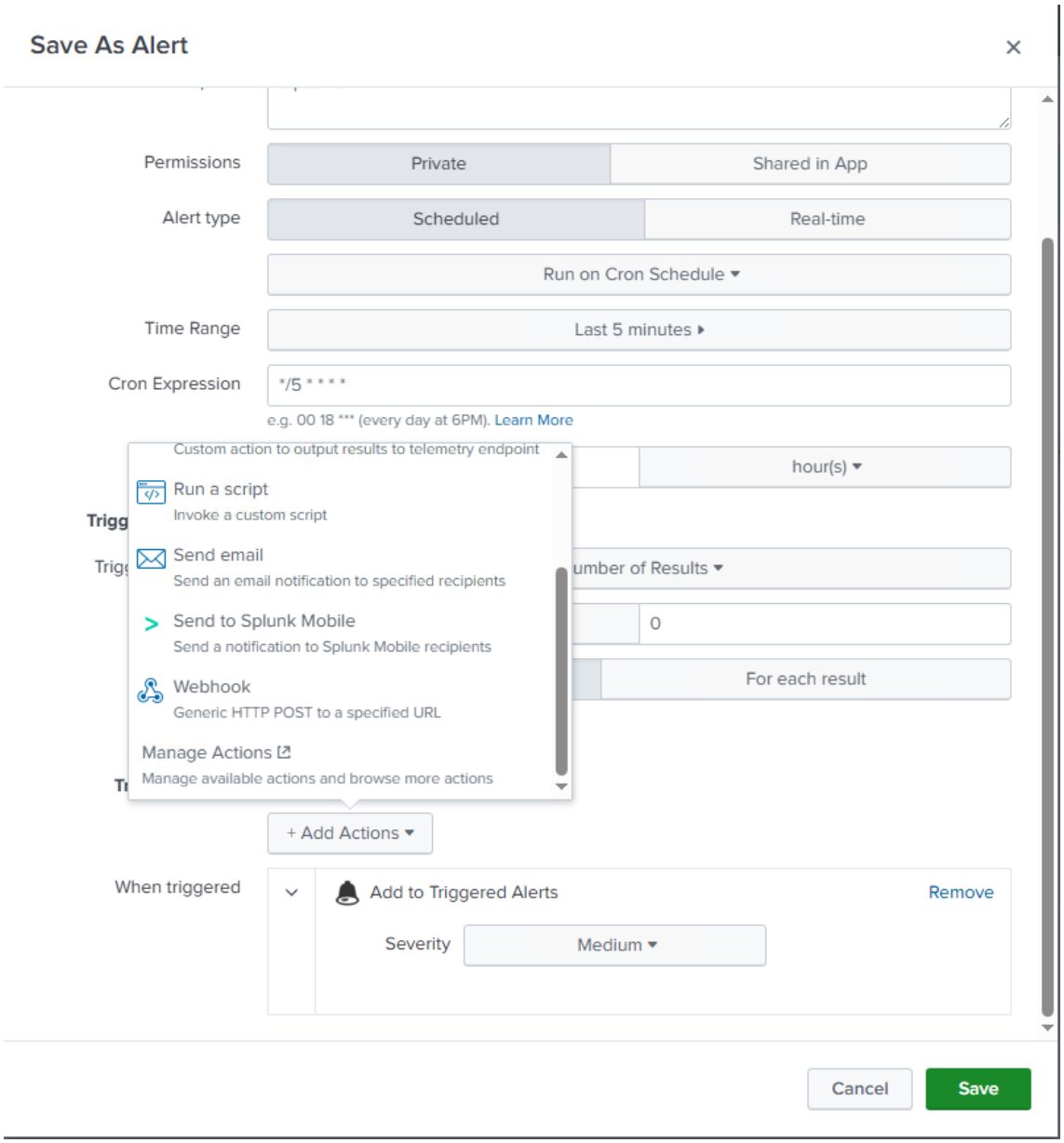


En “Trigger Actions” seleccionamos “+Add Actions” > “Add to Triggered Alerts”.

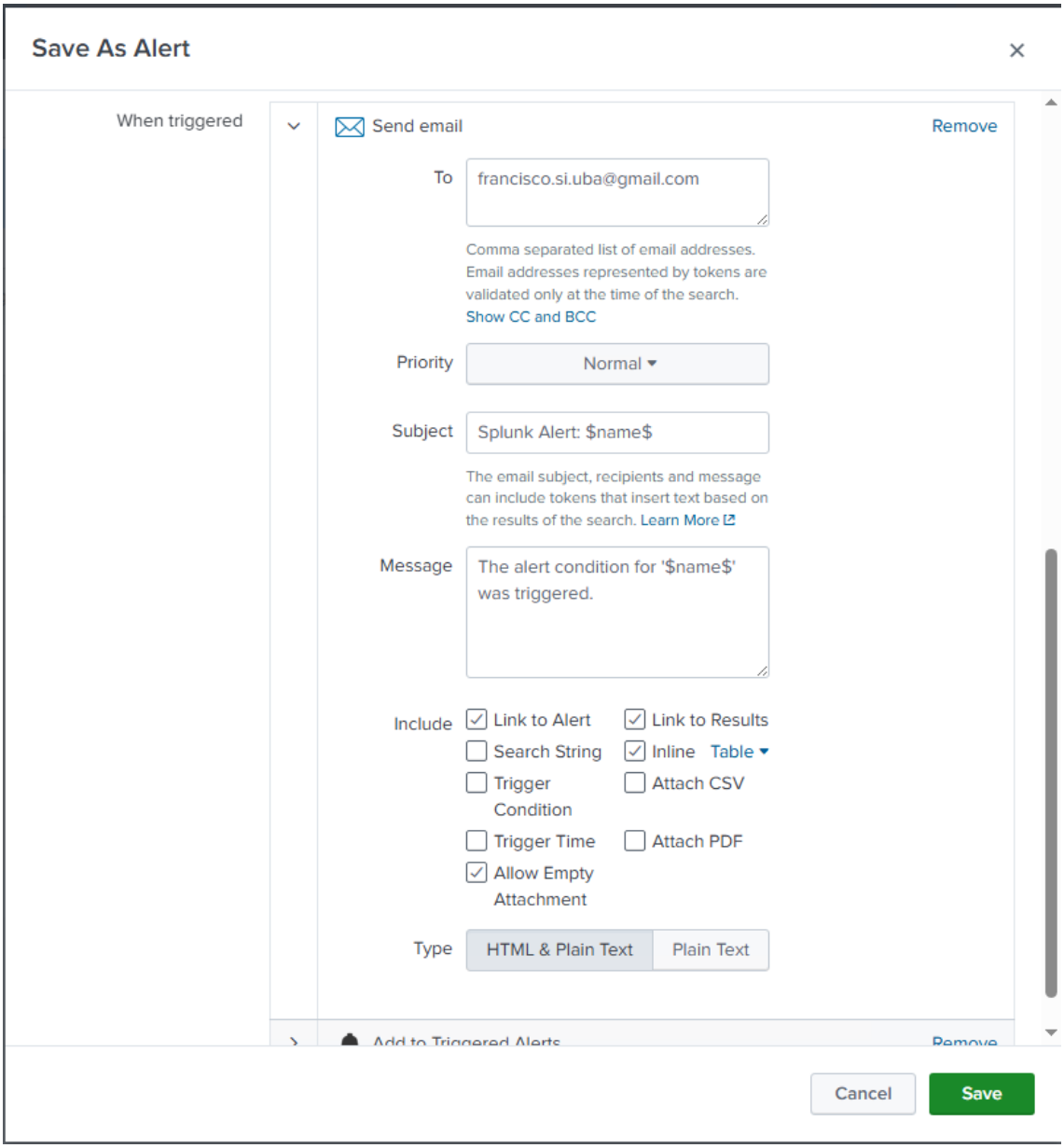
Esto permite que la alerta quede registrada en la plataforma cuando se active.



5. En “Trigger Actions” seleccionamos “+Add Actions” > “Send email”

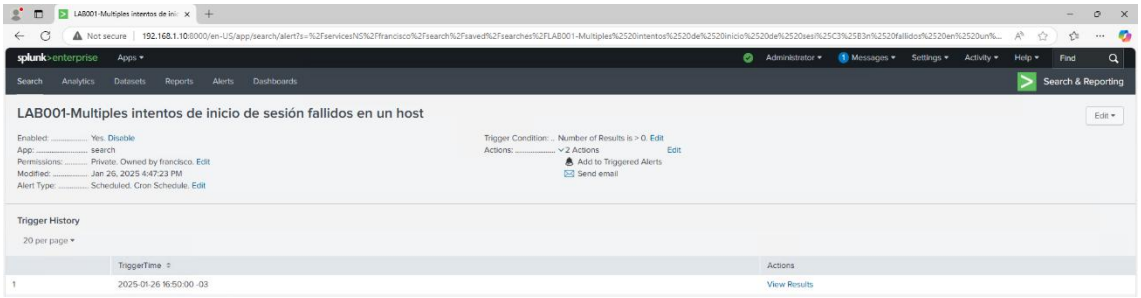


Completamos con el correo destinatario que necesite recibir la alerta.

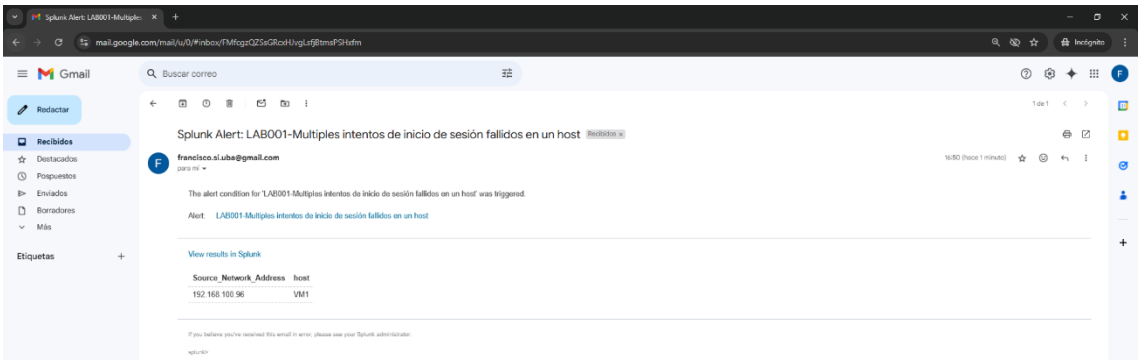


6. Generamos 11 intentos fallidos en menos de 5 minutos y verificamos que se active la alerta en Splunk y su correspondiente recepción de correo.

Alerta en Splunk.



Alerta en correo.

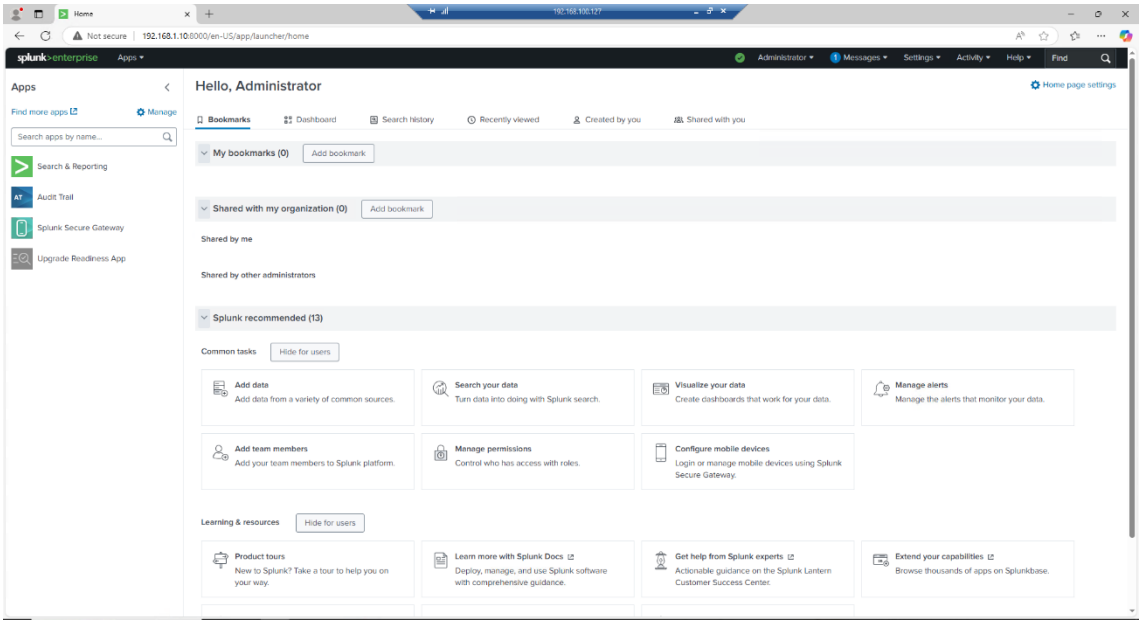


Configuración caso de uso referido a Linux

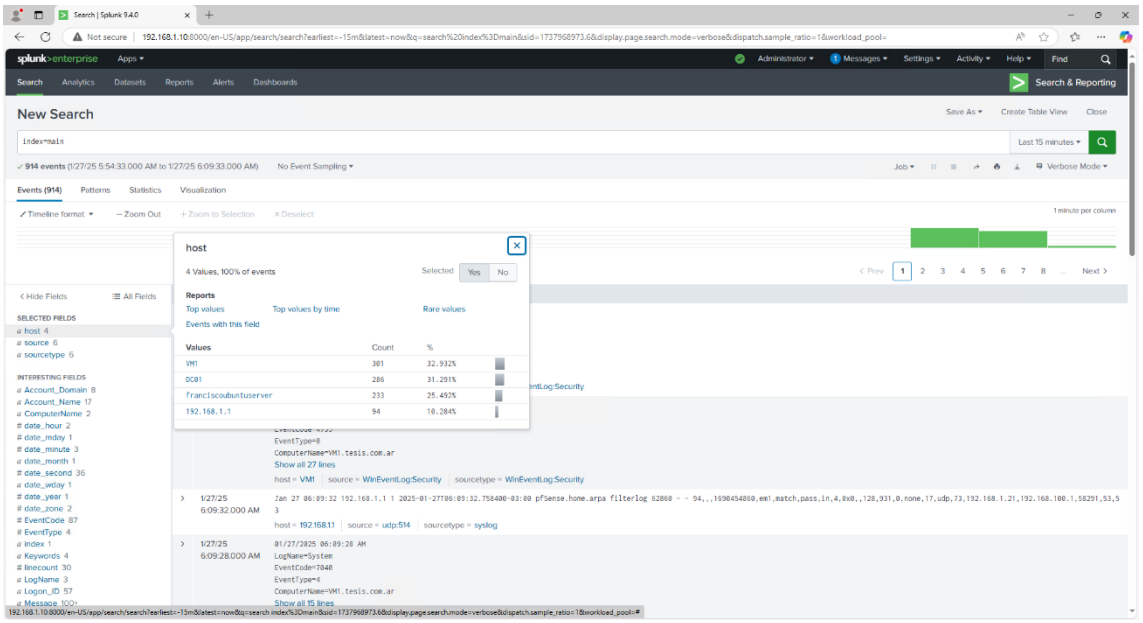
A continuación, se presenta el siguiente caso de uso como ejemplo:

Detectar incorporación de usuarios a grupos privilegiados como “sudo” o “wheel” en servidores Linux.

1. Ingresamos la App de “Seach & Reporting”

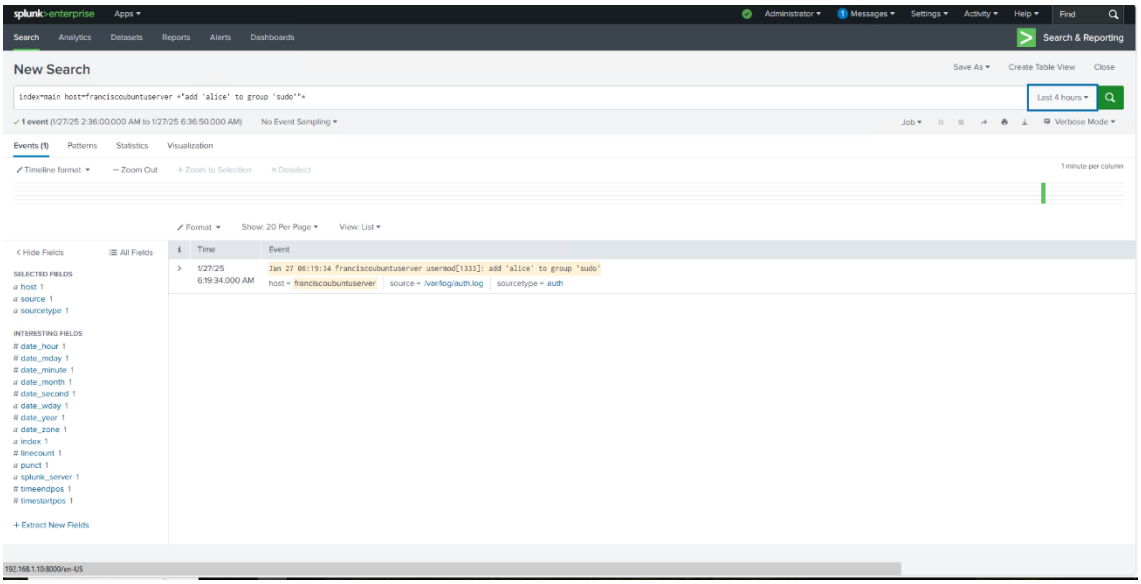


2. En el buscador “Search” realizamos una primera búsqueda especificando el índice que contiene los eventos que estamos buscando.

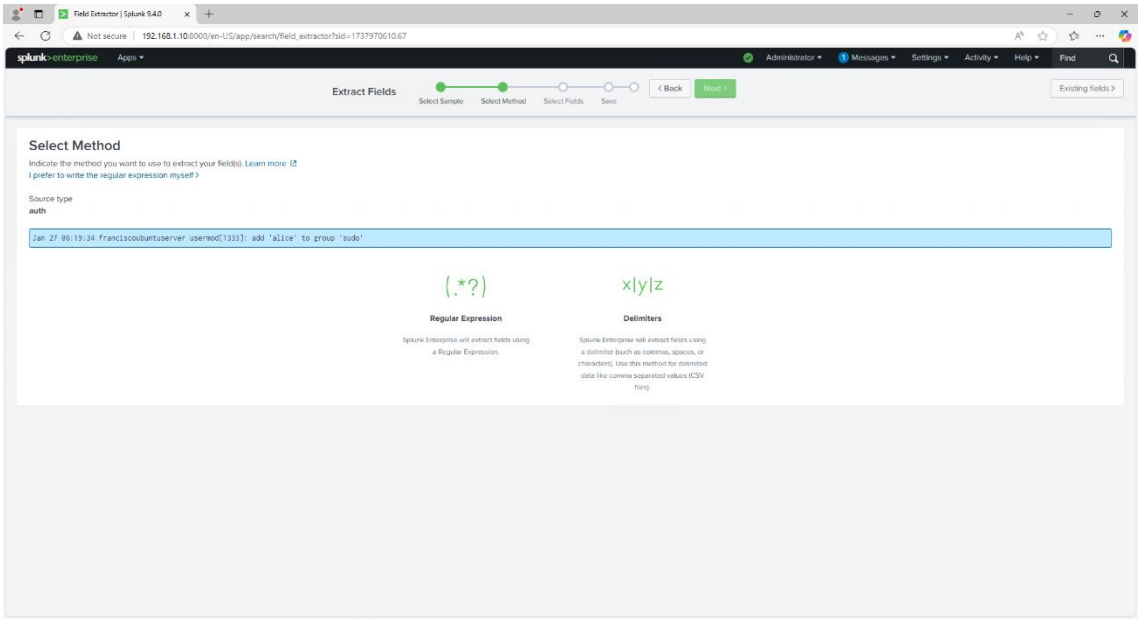


En este caso, ingresamos “index=main” y seleccionamos, dentro de los hosts, a “franciscoubuntuserver”, un servidor que cuenta con un UF instalado y que utilizaremos como referencia para realizar pruebas y desarrollar el caso de uso.

Creo el usuario “alice”, lo agrego al grupo “sudo” en un servidor Ubuntu y, posteriormente, busco el registro correspondiente en Splunk para analizarlo y realizar el parsing. El parsing en Splunk se refiere a tomar los datos crudos de los registros (logs) y estructurarlos en campos clave-valor o secciones que puedan ser fácilmente consultadas, analizadas y visualizadas.



3. Con el evento identificado procedemos a parsear para extraer los campos necesarios, lo que permitirá llevar a cabo búsquedas optimizadas en Splunk.
   Seleccionamos “Extract New Fields”
   Seleccionamos el evento en crudo a utilizar



   Dado que este tipo de eventos no incluye delimitadores específicos como espacios o comas,utilizaremos el método de expresiones regulares para extraer los campos.
   Seleccionamos el valor que deseamos asignar a un campo y le asignamos un nombre, en este caso seleccionamos “alice” y lo etiquetamos como “user_ad_gr”.

Bibliografía

[1] Interpol. [En línea]. Available: https://www.interpol.int/es/content/download/15217/file/20COM0312-Cyberthreats-Campain_ProjectSheet%20-%20SP%20-2020-05.pdf?inLanguage=esl-ES&version=6. [Último acceso: 20 01 2025].

[2] AXUR. [En línea]. Available: https://blog.axur.com/es-es/qu%C3%A9-es-la-fatiga-de-alerta-en-ciberseguridad. [Último acceso: 20 01 2025].

[3] R. Gerhards, 2009. [En línea]. Available: https://dl.acm.org/doi/book/10.17487/RFC5424. [Último acceso: 12 12 2022].

[4] IBM, «IBM - ¿Qué es la gestión de eventos e información de seguridad (SIEM)?,» [En línea]. Available: https://www.ibm.com/mx-es/topics/siem. [Último acceso: 09 12 2023].

[5] A3SEC. [En línea]. Available: https://a3sec.com/blog/siem-2022-cuadrante-magico-de-gartner. [Último acceso: 09 12 2022].

[6] Splunk, «ARQUITECTURAS VALIDADAS DE SPLUNK,» [En línea]. Available: https://www.splunk.com/en_us/pdfs/tech-brief/splunk-validated-architectures-es.pdf. [Último acceso: 09 12 2022].

[7] CrowdStrike. [En línea]. Available: https://www.crowdstrike.com/guides/windows-logging/centralizing-logs/. [Último acceso: 09 12 2022].

[8] Splunk, «Using Syslog-ng with Splunk,» [En línea]. Available: https://www.splunk.com/en_us/blog/tips-and-tricks/using-syslog-ng-with-splunk.html. [Último acceso: 09 12 2022].

[9] Splunk, 10 01 2025. [En línea]. Available: https://www.splunk.com/.

[10] Splunk, «start boot,» [En línea]. Available: https://docs.splunk.com/Documentation/Splunk/9.4.0/Admin/ConfigureSplunktostartatbootime. [Último acceso: 10 01 2025].

[11] Splunk, «UF Windows,» [En línea]. Available: https://docs.splunk.com/Documentation/Forwarder/9.4.0/Forwarder/InstallaWindowsuniversalforwarderfromaninstaller.

[12] Splunk, «UF Linux,» [En línea]. Available: https://docs.splunk.com/Documentation/Forwarder/9.4.0/Forwarder/Installanixuniversalforwarder. [Último acceso: 10 01 2025].

[13] INCIBE, 03 09 2020. [En línea]. Available: https://www.incibe.es/empresas/blog/son-y-sirven-los-siem-ids-e-ips. [Último acceso: 09 12 2023].

[14] J. H. Barrera, 2000. [En línea]. Available: https://ayudacontextos.wordpress.com/wp-content/uploads/2018/04/jacqueline-hurtado-de-barrera-metodologia-de-investigacion-holistica.pdf. [Último acceso: 09 12 2023].