KEEPCODING CIBERSEGURIDAD 9

**PRÁCTICA FINAL ANÁLISIS DE MALWARE**

línea horizontal

# 

### LUIS GÓNGORA - JORDAN DIAZ

**TABLA DE CONTENIDO**

[**PARTE I - INFORME EJECUTIVO**](#_arolcxe0i15c) **3**

[Resumen Ejecutivo](#_la5jp5tnimjw) 3

[Objetivo del proyecto](#_8xa229rzq9tv) 4

[Alcance incluido:](#_9dajnb536q0m) 7

[Resultados Generales](#_pmh95titoghr) 8

[Beneficios Obtenidos](#_r5te5dav80yo) 8

[**PARTE II - INFORME TÉCNICO**](#_oroln3srvyk1) **9**

[Arquitectura del Entorno](#_om4ts3nwb0bh) 9

[Componentes principales](#_vr5bydgwbjf7) 10

[Flujo de datos y procesos](#_xvrcgqwdyamc) 10

[Analisis de Muestras en ANI.RUN](#_sj53l3w9qhqo) 11

[Descripción del proceso](#_nuu6ub3ea7f1) 11

[Procedimiento](#_bn4lxb8qdjh0) 12

[Resultados destacados](#_65ao0i8a3i4m) 12

[Importancia del análisis](#_mong0zti0fj) 13

[Introducción](#_c2pqgutx6psi) 13

[Funcionalidades clave utilizadas](#_98vu3oi0ush9) 14

[Beneficios de la integración](#_5btifs7xf2b1) 14

[Objetivo de la integración](#_m11sz8ai0oeg) 16

[Proceso de integración](#_ppv9gdq4m7br) 16

[Ventajas de esta integración](#_nufh2j6anxjd) 16

[Objetivo](#_k9dgnjh542mi) 18

[Pasos realizados](#_gcpwhkxhqrwz) 18

[Resultados esperados](#_ddyydwaip521) 19

[Objetivo](#_ffwuq2e7yp9x) 20

[Proceso de simulación](#_ut5xd2mvlk3y) 20

[Resultados obtenidos](#_j6hw90kc7pvt) 21

Evidencias………………………………………………………………………………………………………………..22

[Conclusiones](#_luxniiy5vfs2) 23

[Recomendaciones](#_j20ayaly4sa8) 23

# 

# 

# 

# 

# PARTE I - INFORME EJECUTIVO

## Resumen Ejecutivo

El presente proyecto tiene como objetivo demostrar la capacidad de integrar herramientas de análisis de malware y plataformas de gestión de inteligencia de amenazas con sistemas de detección y respuesta en tiempo real. A través de un entorno controlado, se ha desarrollado una solución que permite:

* **Analizar muestras de malware** utilizando Joe Sandbox y Ani.Run para identificar comportamientos maliciosos y extraer indicadores de compromiso (IoCs).
* **Compartir y estructurar la inteligencia** generada a través de una instancia propia de MISP (Malware Information Sharing Platform).
* **Correlacionar eventos y generar alertas** en un SIEM basado en Elastic Cloud, alimentado tanto por los IoCs de MISP como por datos recogidos desde una máquina Windows infectada con un agente ELK.

El flujo completo reproduce una situación real de infección, análisis, generación de inteligencia, detección y respuesta, lo que permite ilustrar cómo las organizaciones pueden automatizar procesos de ciberseguridad utilizando herramientas abiertas y ampliamente utilizadas en el sector.

Este entorno no solo permite reforzar el conocimiento técnico adquirido durante el bootcamp, sino que también ofrece una visión integral de cómo un SOC moderno puede integrar inteligencia de amenazas para detectar compromisos de forma eficaz y oportuna.

## 

## 

## Objetivo del proyecto

El objetivo principal de este proyecto es diseñar y desplegar un entorno funcional para el **análisis, gestión de inteligencia de amenazas y detección de compromisos mediante alertas automatizadas**, utilizando herramientas ampliamente reconocidas en el ámbito de la ciberseguridad.

De forma más específica, el proyecto busca:

* **Analizar muestras de malware** en un entorno aislado, con el fin de identificar comportamientos maliciosos y extraer indicadores de compromiso (IoCs).
* **Integrar la inteligencia generada** en una plataforma MISP autogestionada, permitiendo su organización, almacenamiento y reutilización como conocimiento compartido.
* **Implementar un sistema SIEM basado en Elastic Cloud**, capaz de consumir los indicadores de MISP y monitorear en tiempo real los eventos de una máquina Windows con un agente ELK.
* **Simular una infección en la máquina Windows** y comprobar que los eventos generados permiten la detección y respuesta ante el compromiso.
* **Demostrar un flujo completo de trabajo** que conecta el análisis de amenazas con la detección efectiva mediante herramientas open source y entornos en la nube.

Este enfoque integral permite no solo identificar y documentar amenazas, sino también responder activamente mediante correlación de eventos y alertas automáticas, alineándose con los principios fundamentales de un Centro de Operaciones de Seguridad (SOC).

1. **Justificación**

En un entorno donde las amenazas informáticas evolucionan constantemente, la detección temprana y la respuesta efectiva ante incidentes se han convertido en pilares fundamentales de la ciberseguridad moderna. Las organizaciones necesitan soluciones que les permitan identificar comportamientos anómalos, correlacionar eventos y actuar de forma automatizada y eficiente.

Este proyecto se justifica por los siguientes motivos clave:

* **Creciente sofisticación del malware:** Hoy en día, muchas amenazas son capaces de evadir controles tradicionales. Es imprescindible analizar su comportamiento dinámico para comprender sus tácticas, técnicas y procedimientos (TTP).
* **Necesidad** **de inteligencia accionable:** No basta con detectar un malware, también es crucial generar, estructurar y compartir inteligencia que permita prevenir futuras infecciones. MISP facilita esta labor como plataforma centralizada de (IoCs) y conocimiento.
* **Relevancia de los sistemas SIEM en entornos reales:** Un SIEM bien configurado permite una visibilidad completa sobre lo que ocurre en una red, integrando múltiples fuentes de datos. Elastic SIEM, en particular, representa una solución flexible, escalable y asequible para muchos entornos.
* **Conexión entre análisis ofensivo y defensa activa:** Este entorno reproduce un ciclo completo donde se parte de una amenaza (análisis) y se concluye con su detección (defensa), replicando flujos que se utilizan en equipos Red y Blue Team.
* **Aplicabilidad real:** Todas las herramientas utilizadas son de uso profesional y están activamente implementadas en organizaciones del sector público y privado, lo que refuerza la validez del proyecto como ejercicio práctico de alto valor.

En conjunto, este proyecto permite demostrar cómo una infraestructura de bajo coste basada en tecnologías abiertas puede convertirse en una solución potente para la gestión de amenazas y la defensa proactiva en entornos reales.

1. **Alcance del Proyecto**

El presente proyecto abarca el diseño, despliegue y validación de un entorno integral para el análisis de malware, la gestión de inteligencia de amenazas y la detección de compromisos mediante alertas automatizadas. El alcance se divide en varios componentes interconectados:

### Alcance incluido:

* **Instalación y configuración de una máquina virtual con MISP**, utilizada como repositorio centralizado de indicadores de compromiso (IoCs).
* **Análisis dinámico de varias muestras de malware** utilizando Joe Sandbox (versión cloud) y Ani.Run, permitiendo observar su comportamiento y extraer indicadores relevantes.
* **Exportación e importación de IoCs** desde Joe Sandbox y Ani.Run a MISP, incluyendo hashes, nombres de archivos, direcciones IP, URLs y claves de registro maliciosas.
* **Integración de MISP con Elastic Cloud SIEM**, utilizando feeds para consumir inteligencia de amenazas directamente desde la plataforma.
* **Despliegue de una máquina virtual Windows con agente Elastic (Winlogbeat/Filebeat/Elastic Agent)** para monitorizar eventos y simular un sistema víctima.
* **Simulación de infección en el sistema Windows** y validación de alertas generadas en el SIEM.
* **Visualización y análisis de los eventos de seguridad en Kibana**, incluyendo dashboards, reglas de correlación y alertas.

Este alcance permite una cobertura completa del ciclo de detección de amenazas a partir del análisis de malware, desde la generación de inteligencia hasta la detección en un entorno simulado, demostrando su aplicabilidad práctica en entornos reales.

1. **Resultados Generales y Beneficios**

### Resultados Generales

Durante la ejecución del proyecto se logró implementar con éxito una arquitectura funcional compuesta por herramientas clave del ecosistema de ciberseguridad:

* Se desplegó una instancia operativa de **MISP**, permitiendo importar, organizar y visualizar inteligencia de amenazas generada a partir del análisis dinámico de malware.
* Se realizó un **análisis detallado de varias muestras maliciosas** en Joe Sandbox y Ani.Run, extrayendo indicadores de compromiso relevantes (hashes, dominios, direcciones IP, archivos, claves de registro, etc.).
* Se configuró la **integración entre MISP y Elastic Cloud SIEM**, logrando que los indicadores sean consumidos automáticamente para su correlación con los eventos del sistema monitorizado.
* Se desplegó una **máquina virtual Windows simulando una víctima**, equipada con el agente de Elastic para recolectar y enviar eventos en tiempo real.
* Tras simular la infección, se logró la **detección de la actividad maliciosa** mediante reglas de correlación y alertas en Kibana, validando el flujo completo desde la amenaza hasta su identificación.

### Beneficios Obtenidos

* **Automatización del ciclo de respuesta ante amenazas**, desde el análisis inicial hasta la generación de alertas.
* **Centralización de la inteligencia de amenazas** mediante MISP, facilitando la reutilización y el enriquecimiento de IoCs.
* **Demostración práctica del valor de un SIEM** en la detección temprana de compromisos.
* **Fortalecimiento del enfoque defensivo**, alineado con buenas prácticas del modelo SOC (Security Operations Center).
* **Aprendizaje técnico transversal**, combinando conocimientos de análisis de malware, threat intelligence, arquitectura SIEM y administración de sistemas.

Este entorno ha demostrado ser una solución eficaz, flexible y económica para entornos educativos, laboratorios de investigación o incluso pequeñas organizaciones que desean implementar un flujo de detección y análisis de amenazas sin necesidad de grandes inversiones.

# PARTE II - INFORME TÉCNICO

## Arquitectura del Entorno

El proyecto se basa en una arquitectura modular e integrada que permite el análisis, gestión y detección de malware mediante el uso combinado de herramientas especializadas y una plataforma de monitoreo centralizada.

### Componentes principales

* **Máquina Virtual con MISP (Malware Information Sharing Platform):** Servidor dedicado para la gestión y almacenamiento de inteligencia de amenazas. En esta plataforma se importan y organizan los indicadores extraídos durante el análisis de malware, facilitando su compartición y reutilización.
* **ANI.RUN (Análisis Dinámico de Malware):** Herramienta en la nube que permite ejecutar las muestras maliciosas en un entorno controlado para observar su comportamiento, incluyendo creación de procesos, conexiones de red, modificaciones en el sistema, etc. Los resultados obtenidos generan IoCs que son exportados a MISP.
* **Elastic Cloud SIEM:** Plataforma de monitoreo y análisis de seguridad basada en la suite Elastic (Elasticsearch, Kibana y Beats). Se configura para consumir los IoCs desde MISP, además de recolectar eventos desde los agentes instalados en los sistemas monitorizados.
* **Máquina Virtual Windows con agente Elastic:** Sistema objetivo donde se simula la infección. El agente instalado (Winlogbeat, Filebeat o Elastic Agent) recolecta logs de eventos del sistema operativo, procesos y conexiones de red, enviándolos al SIEM para su análisis y correlación.

### Flujo de datos y procesos

* La muestra de malware es analizada en ANI.RUN, donde se obtiene un reporte detallado de comportamiento y se extraen indicadores de compromiso (hashes, URLs, IPs, claves de registro, etc.).
* Estos indicadores son exportados e importados a MISP, donde se estructuran y almacenan para su posterior consumo.
* Elastic Cloud SIEM consulta periódicamente a MISP para obtener los indicadores más recientes, creando listas de IoCs para detectar actividad sospechosa en la red o en los endpoints.
* La máquina Windows infectada genera eventos en tiempo real que son enviados por el agente Elastic al SIEM.
* El SIEM correlaciona los eventos entrantes con los IoCs provenientes de MISP, disparando alertas cuando se detectan coincidencias, lo que permite una respuesta rápida ante posibles compromisos.

## **Analisis de Muestras en ANI.RUN**

### Descripción del proceso

Para comprender el comportamiento del malware y obtener indicadores útiles para su detección, se utilizó la plataforma ANI.RUN, una herramienta avanzada de análisis dinámico que permite ejecutar muestras en un entorno aislado y controlado.

### Procedimiento

* Se cargó la muestra maliciosa en ANI.RUN y se configuró para realizar un análisis profundo del comportamiento en Windows.
* La plataforma ejecutó la muestra y monitoreó diversas actividades, incluyendo:  
  + Creación y modificación de archivos.
  + Cambios en el registro de Windows.
  + Comunicación de red (conexiones HTTP, DNS, IPs).
  + Creación y ejecución de procesos secundarios.
  + Técnicas anti-análisis o evasión.

### Resultados destacados

* **Hashes identificados:** Se obtuvieron los valores MD5, SHA1 y SHA256 de la muestra, confirmando su integridad y permitiendo su rastreo.
* **Indicadores de compromiso (IoCs):**
  + Direcciones IP y dominios utilizados para comunicación C2.
  + URLs sospechosas y patrones de tráfico HTTP anómalos.
  + Archivos creados o modificados, incluyendo notas de rescate y ejecutables temporales.
  + Claves de registro alteradas para persistencia y ejecución automática.
* **Comportamiento observable:**
  + Ejecución de comandos para eliminar copias de seguridad y borrar evidencia.
  + Modificación de archivos de usuario y robo de información sensible.
  + Intentos de conexión a la red TOR para ocultar comunicación.

### Importancia del análisis

Este análisis permitió obtener un conjunto robusto de indicadores que alimentan la plataforma MISP, habilitando una defensa basada en inteligencia que facilita la detección temprana y la respuesta oportuna ante ataques similares.

1. **Gestión e Integración de Inteligencia en MISP**

### Introducción

MISP (Malware Information Sharing Platform) es una plataforma de código abierto diseñada para facilitar la recopilación, almacenamiento, distribución y análisis de información relacionada con amenazas y malware. Su integración en el proyecto permite centralizar y estructurar la inteligencia obtenida durante el análisis dinámico.

### Funcionalidades clave utilizadas

* **Importación de Indicadores de Compromiso (IoCs):** Los indicadores extraídos desde ANI.RUN, tales como hashes, URLs, direcciones IP, nombres de archivos y claves de registro, fueron importados a MISP para su almacenamiento organizado.
* **Clasificación y etiquetado:** MISP permite clasificar los IoCs mediante taxonomías y etiquetas, facilitando la búsqueda, correlación y análisis contextual de la información.
* **Relaciones entre eventos:** Los distintos IoCs se relacionan entre sí para construir un panorama completo del comportamiento del malware y sus vectores de ataque.
* **Exportación y consumo de inteligencia:** MISP genera feeds actualizados que pueden ser consultados por herramientas externas, como un SIEM, para automatizar la detección basada en inteligencia.

### Beneficios de la integración

* **Centralización del conocimiento:** La plataforma ofrece un repositorio único y estructurado que facilita el trabajo colaborativo y la reutilización de la inteligencia.
* **Actualización continua:** Los indicadores pueden ser actualizados y enriquecidos a medida que se obtienen nuevos hallazgos o se detectan variantes.
* **Interoperabilidad:** Gracias a sus APIs y formatos estándares (STIX, OpenIOC), MISP se integra fácilmente con sistemas de detección y respuesta.

1. **Integración de MISP con Elastic Cloud SIEM**

### Objetivo de la integración

La integración entre MISP y Elastic Cloud SIEM busca automatizar la ingestión y correlación de indicadores de compromiso (IoCs) dentro de la plataforma de monitoreo para facilitar la detección temprana de amenazas y mejorar la capacidad de respuesta ante incidentes.

### Proceso de integración

* **Exportación de IoCs desde MISP:** MISP genera feeds de inteligencia en formatos compatibles, que incluyen listas actualizadas de hashes, dominios, URLs, direcciones IP y otros indicadores relevantes.
* **Configuración en Elastic Cloud SIEM:** Se implementan reglas y módulos específicos para consumir estos feeds directamente desde MISP, permitiendo que el SIEM mantenga listas de IoCs actualizadas de forma automática.
* **Correlación de eventos:** Elastic SIEM recibe datos de los endpoints (como logs de Windows, conexiones de red, procesos, etc.) y compara esta información con los indicadores provenientes de MISP.
* **Generación de alertas:** Cuando se detecta alguna coincidencia entre eventos reales y los IoCs, el SIEM dispara alertas configuradas para notificar a los equipos de seguridad y permitir una acción rápida.

### Ventajas de esta integración

* **Detección proactiva:** Al disponer de inteligencia actualizada, se mejora la capacidad para detectar compromisos antes de que causen daños mayores.
* **Automatización:** Reduce la intervención manual para actualizar listas de amenazas, optimizando tiempos y recursos del equipo de seguridad.
* **Visibilidad consolidada:** Elastic SIEM ofrece paneles visuales (dashboards) donde se pueden monitorear en tiempo real las amenazas detectadas basadas en inteligencia externa.

1. **Configuración de la Máquina de Windows con agente ELK**

### Objetivo

Configurar un sistema operativo Windows como endpoint monitorizado, instalando y configurando los agentes de Elastic para recolectar y enviar logs y eventos de seguridad hacia Elastic Cloud SIEM, facilitando así la detección y análisis de incidentes.

### Pasos realizados

* **Preparación del entorno Windows:**
  + Instalación del sistema operativo Windows en una máquina virtual configurada para pruebas.
  + Configuración básica de red y seguridad para permitir la comunicación con Elastic Cloud.
* **Instalación del Elastic Agent:**
  + Descarga e instalación del Elastic Agent, que centraliza la recolección de datos en lugar de utilizar agentes individuales como Winlogbeat o Filebeat.
  + Configuración inicial para conectar el agente con la instancia de Elastic Cloud SIEM mediante la URL y las credenciales adecuadas.
* **Configuración de módulos y políticas:**
  + Aplicación de políticas específicas en Elastic Cloud para la recolección de eventos de seguridad de Windows, incluyendo logs de sistema, aplicaciones y seguridad.
  + Activación de módulos adicionales para captura de eventos de red, procesos y archivos.
* **Validación de la conectividad:**
  + Confirmación mediante Kibana que los eventos generados por la máquina Windows llegan correctamente al SIEM en tiempo real.

### Resultados esperados

* Captura continua y fiable de logs relevantes para la seguridad.
* Disponibilidad de información detallada para correlacionar eventos con indicadores provenientes de MISP.
* Facilidad para generar alertas y dashboards personalizados que reflejen el estado de seguridad del endpoint.

1. **Simulación de Infección y Detección de alertas**

### Objetivo

Validar el entorno completo implementado realizando una simulación controlada de infección en la máquina Windows con la muestra de malware analizada, y observar la generación de alertas en Elastic Cloud SIEM.

### Proceso de simulación

* **Ejecución de la muestra maliciosa:**
  + La muestra analizada previamente se ejecutó en la máquina Windows configurada con el agente Elastic, replicando el comportamiento observado en ANI.RUN.
* **Monitoreo de eventos:**
  + El agente Elastic recolectó logs y eventos generados durante la ejecución del malware, incluyendo creación/modificación de archivos, conexiones de red y cambios en el registro.
* **Correlación en Elastic Cloud SIEM:**
  + Los eventos fueron correlacionados con los indicadores importados desde MISP.
  + Se activaron reglas de detección configuradas para identificar actividad maliciosa basada en IoCs.
* **Generación de alertas:**
  + Se dispararon alertas específicas dentro del SIEM notificando la detección de actividad sospechosa relacionada con la muestra.
  + Se validó que las alertas contenían información suficiente para la identificación rápida y la respuesta.

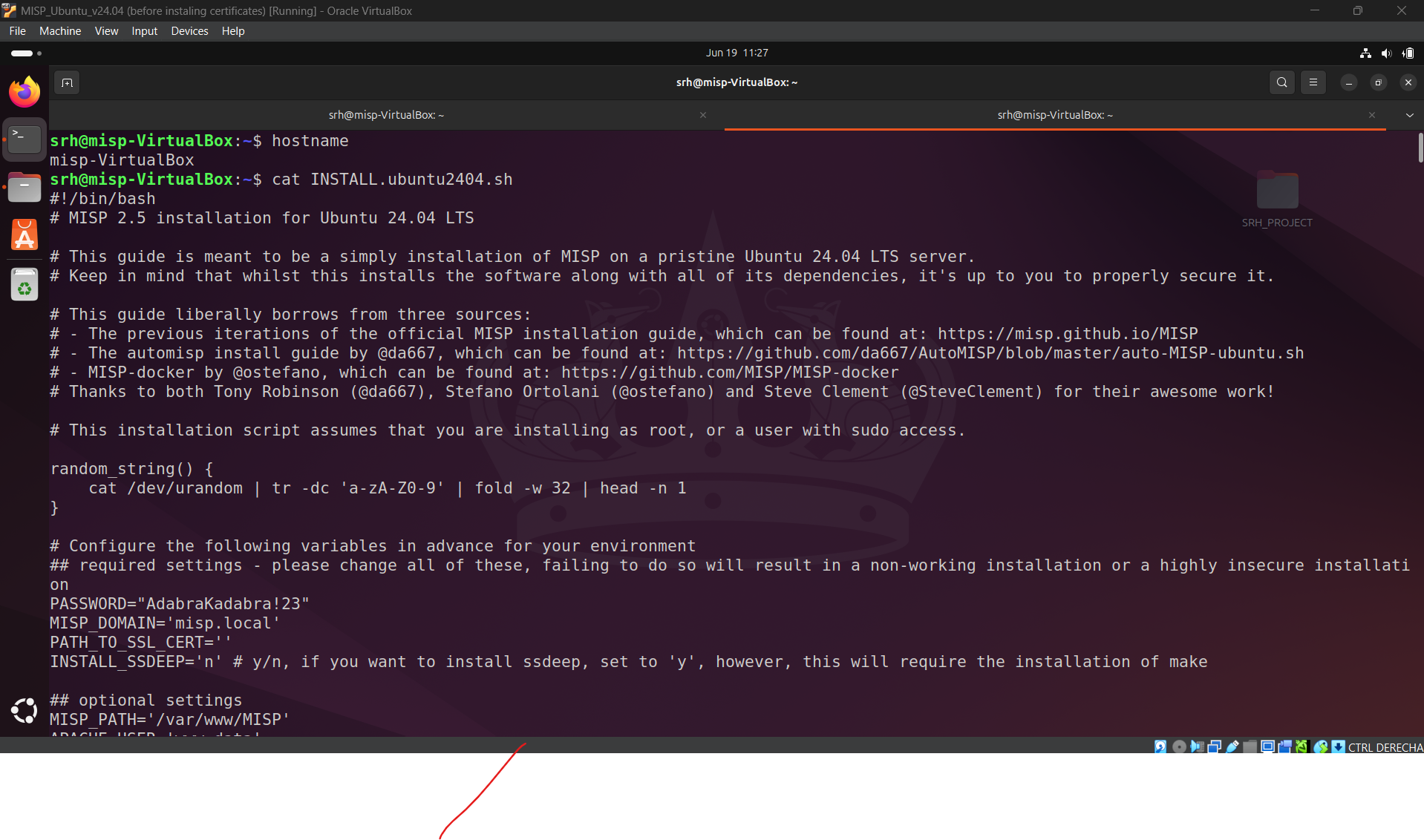
### Resultados obtenidos

* Confirmación de la correcta ingestión y correlación de datos entre los diferentes componentes.
* Validación del flujo de análisis, inteligencia y detección en un entorno controlado.
* Evidencia del valor práctico de la integración para mejorar la visibilidad y la capacidad de respuesta ante amenazas reales.

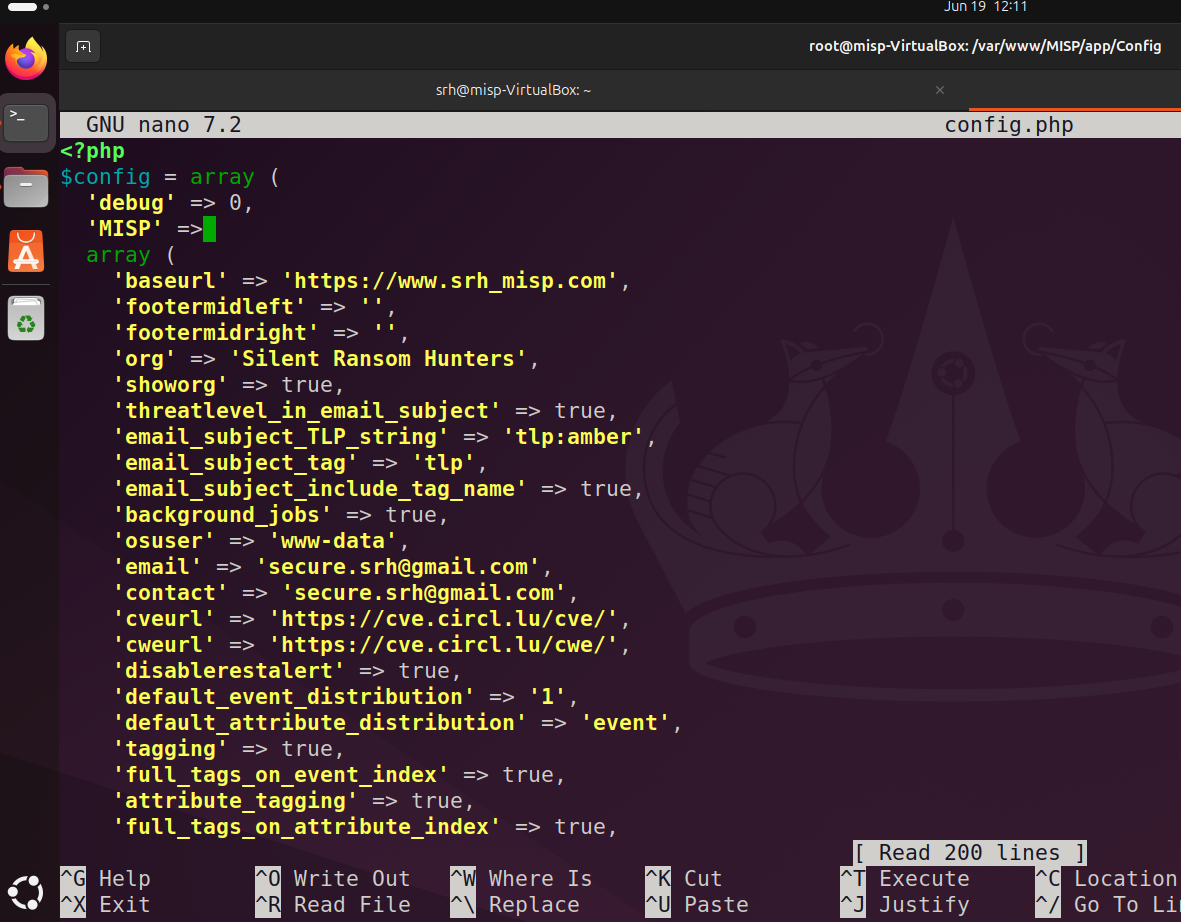
1. **Evidencias**

**Misp**

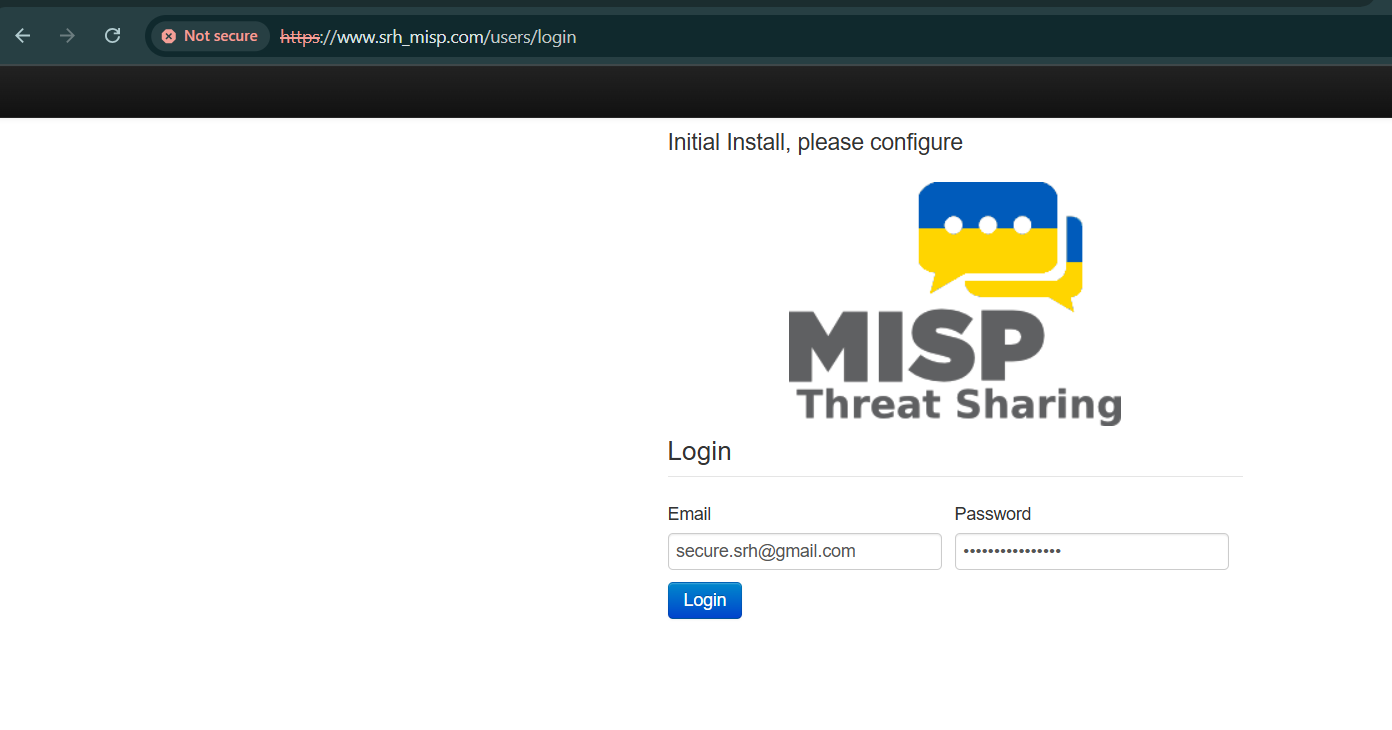
Se configura el script [INSTALL.ubuntu.2404.sh](https://github.com/MISP/MISP/tree/2.5/INSTALL) obtenido del repositorio GitHub de Misp para proceder con su instalación.

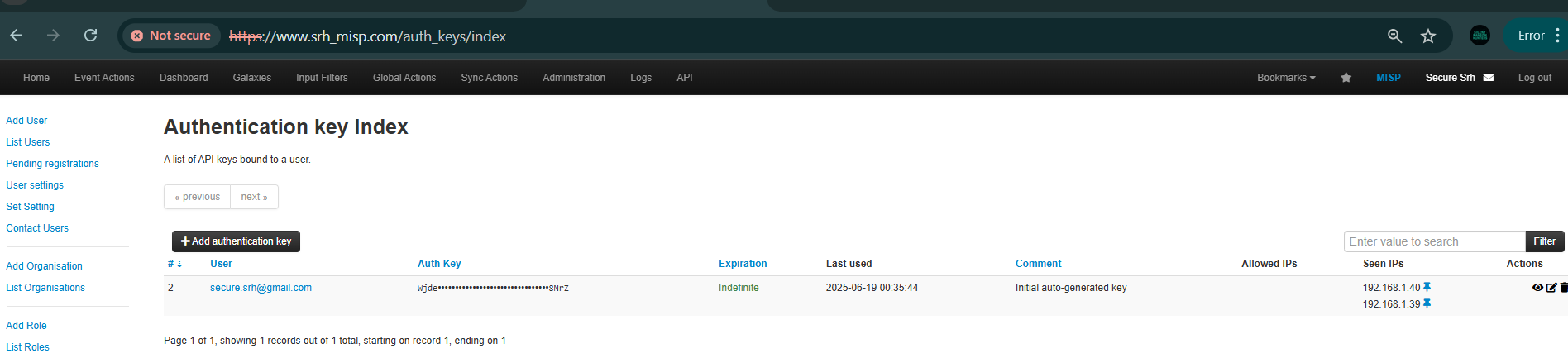
****

Se establece toda la configuración necesaria para su funcionamiento

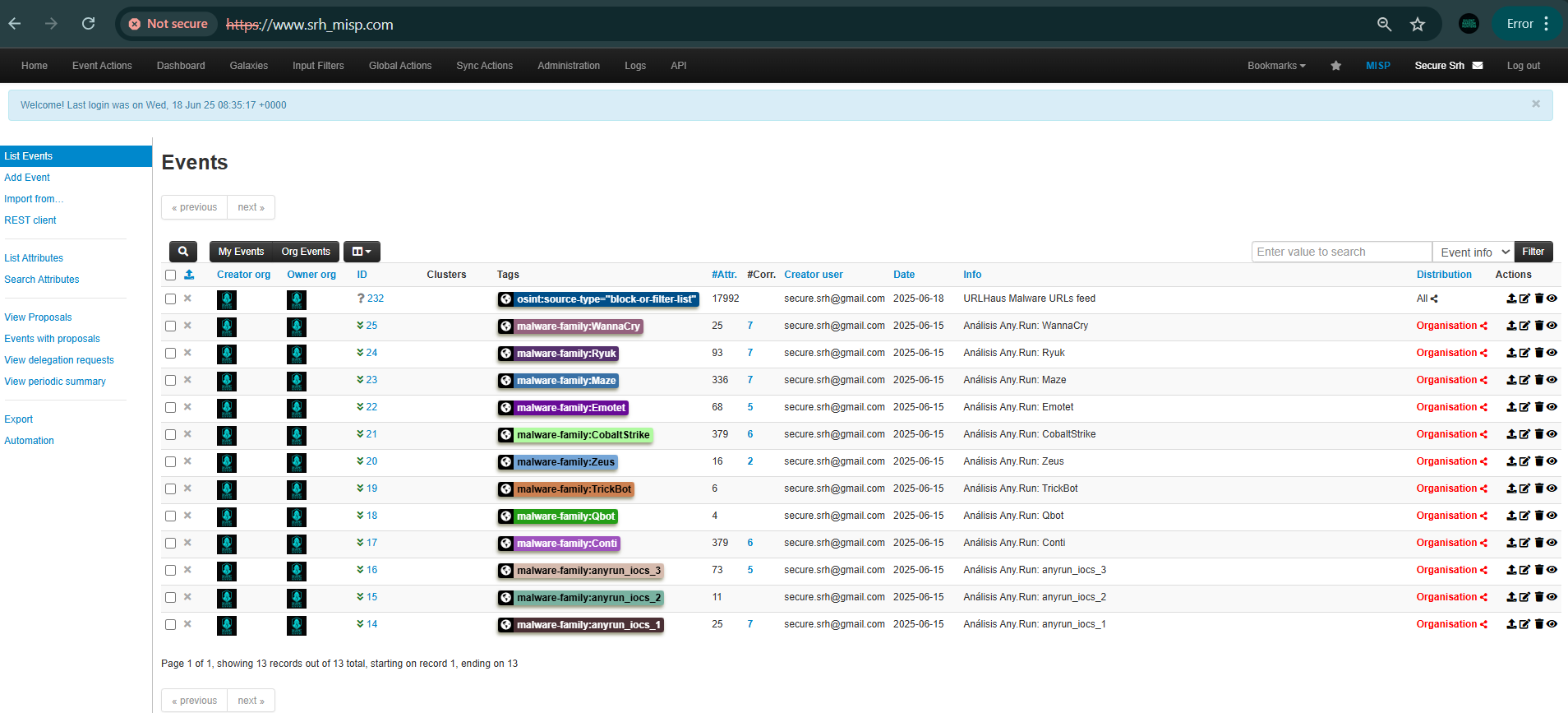
****

Configuramos el nombre DNS junto con la IP en el archivo **/etc/hosts** de la VM y accedemos a la interfaz web ya configurada.

  
Se genera una **API key** para sus futuras integraciones con **ELK.**

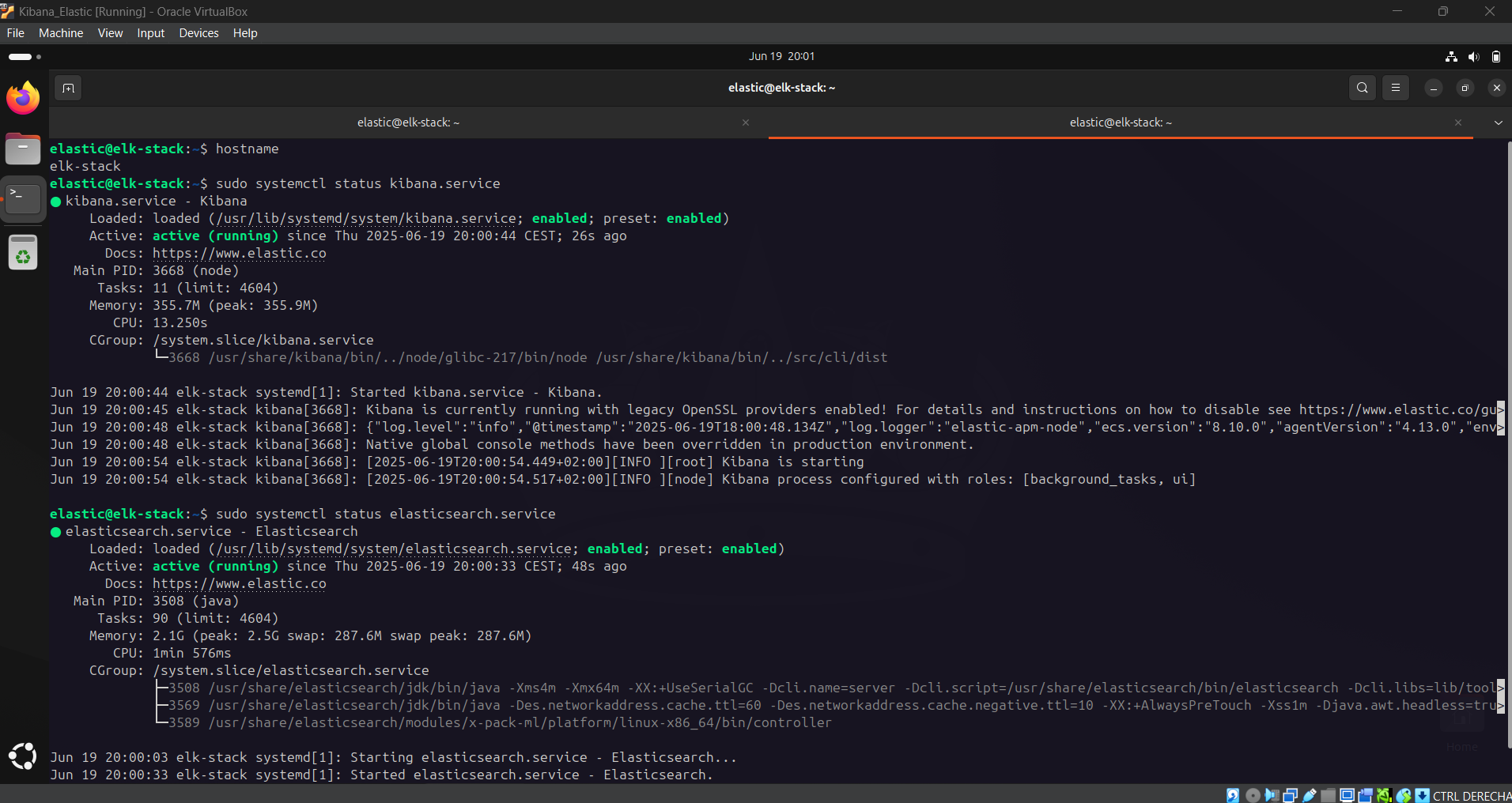
****

Se descargan las 12 IOCs desde **ANY.RUN** y se cargan en **Misp** mediante scriptpara su posterior enriquecimiento.

****

**Elastic stack**

Instalación y puesta en marcha de Elastic Stack (también conocido como ELK Stack)

****

**Conclusiones y Recomendaciones**

### Conclusiones

* Se demostró la viabilidad de integrar herramientas especializadas de análisis de malware, inteligencia de amenazas y monitoreo de seguridad para construir un sistema eficiente de detección y respuesta.
* La plataforma MISP resultó fundamental para centralizar y organizar los indicadores de compromiso, facilitando su consumo automático por parte de Elastic Cloud SIEM.
* La configuración del agente Elastic en la máquina Windows permitió la recolección en tiempo real de eventos, habilitando la correlación inmediata con la inteligencia importada.
* La simulación de infección confirmó que el sistema puede detectar actividades maliciosas y generar alertas oportunas, lo que es crucial para reducir tiempos de respuesta y mitigar riesgos.
* Este proyecto evidencia cómo un entorno integrado y automatizado puede fortalecer las capacidades de seguridad incluso en organizaciones con recursos limitados.

### Recomendaciones

* **Mantener actualizada la inteligencia:** Continuar importando indicadores frescos en MISP para asegurar la detección de nuevas amenazas.
* **Optimizar reglas y alertas:** Ajustar las reglas del SIEM para reducir falsos positivos y mejorar la precisión.
* **Capacitación continua:** Formar al equipo de seguridad en el uso de las herramientas y en la interpretación de alertas.
* **Implementar respuesta automatizada:** Considerar la incorporación de sistemas SOAR para automatizar acciones frente a incidentes detectados.
* **Ampliar el monitoreo:** Extender la recolección de datos a más endpoints y fuentes para aumentar la cobertura y visibilidad.