Maestría en

CIBERSEGURIDAD

Trabajo previo a la obtención de título de
Magister en Ciberseguridad

AUTOR/ES:

Aguilar Reasco Martha Melany

Arévalo Moreira Rommel Francisco

Calvopiña Tipan Steve Alexander

Parrales Cabrera Geoconda Daniela

TUTORES:

Iván Reyes Chacón

Paulina Vizcaíno

Tema: Implementación de un Sistema Honeypot en Microsoft Azure con Ingesta y Correlación de Eventos Mediante Sentinel para el Fortalecimiento de la Detección Temprana y Proactiva de Eventos.

Quito - Ecuador

Junio – 2026

REINVENTEMOS EL FUTURO

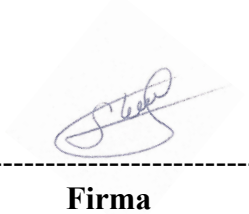
Certificación de autoría

Nosotros, Aguilar Reasco Martha Melany, Arévalo Moreira Rommel Francisco, Calvopiña Tipan Steve Alexander, Parrales Cabrera Geoconda Daniela, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido presentado anteriormente para ningún grado o calificación profesional y que se ha consultado la bibliografía detallada.

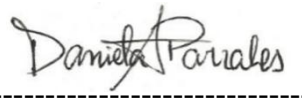
Cedemos nuestros derechos de propiedad intelectual a la Universidad Internacional del Ecuador (UIDE), para que sea publicado y divulgado en internet, según lo establecido en la Ley de Propiedad Intelectual, su reglamento y demás disposiciones legales.

Firma
Aguilar Reasco Martha Melany

Firma
Arévalo Moreira Rommel Francisco



Firma
Calvopiña Tipan Steve Alexander



Firma
Parrales Cabrera Geoconda Daniela

Autorización de Derechos de Propiedad Intelectual

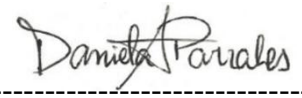
Nosotros, Aguilar Reasco Martha Melany, Arévalo Moreira Rommel Francisco, Calvopiña Tipan Steve Alexander, Parrales Cabrera Geoconda Daniela en calidad de autores del trabajo de investigación titulado ***Titulo del trabajo de investigación: Implementación de un Sistema Honeypot en Microsoft Azure con Ingesta y Correlación de Eventos Mediante Sentinel para el Fortalecimiento de la Detección Temprana y Proactiva de Eventos***, autorizamos a la Universidad Internacional del Ecuador (UIDE) para hacer uso de todos los contenidos que nos pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación. Los derechos que como autores nos corresponden, lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

D. M. Quito, Julio 2026

Firma
Aguilar Reasco Martha Melany

Firma
Arévalo Moreira Rommel Francisco

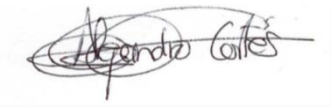
Firma
Calvopiña Tipan Steve Alexander



Firma
Parrales Cabrera Geoconda Daniela

Aprobación de dirección y coordinación del programa

Nosotros, **Alejandro Cortés y Ivan Reyes**, declaramos que**: Aguilar Reasco Martha Melany, Arévalo Moreira Rommel Francisco, Calvopiña Tipan Steve Alexander, Parrales Cabrera Geoconda Daniela** son los autores exclusivos de la presente investigación y que ésta es original, auténtica y personal de ellos.



Alejandro Cortés
Director/a de la
Maestría en Ciberseguridad

Iván Reyes
Coordinador/a de la
Maestría en Ciberseguridad

Dedicatoria / Agradecimientos

Quiero dedicar este trabajo a Dios, por darme la fortaleza y sabiduría para culminar esta etapa. A mi familia y seres queridos, por su apoyo incondicional, paciencia y aliento constante a lo largo de este camino. Este logro es tan suyo como mío.

Aguilar Reasco Martha Melany

Dedico este trabajo a mis padres que son mi fuente de inspiración y mi motor, con ustedes ningún reto es demasiado grande. A Alexandra, Alberto y en especial a Ronald espero que su cariño y su recuerdo sean atemporales.

Arévalo Moreira Rommel Francisco

Este trabajo se lo dedico a mis padres, ambos me han apoyado toda mi vida y les debo todo, no solo lo económico y material ustedes me han formado en la persona que soy ahora y aunque quizás nunca pueda pagarles todo eso, espero que este título les pueda hacer sentirse tan orgullosos de ser mis padres, como yo me siento de ser su hijo.

También se lo dedico a mi abuelita que me acompaño en cada paso de mi vida universitaria acompañándome en los mejores y peores momentos de este camino realmente usted mami se merece todo, los amo un mundo a los tres.

Steve Alexander Calvopiña Tipan

Dedico el presente trabajo a Dios, por brindarme la fortaleza y la sabiduría necesarias para culminar esta etapa de mi vida. A mi familia, por su apoyo incondicional, comprensión y motivación constante a lo largo de este proceso académico.

Parrales Cabrera Geoconda Daniela

RESUMEN

Esta investigación aborda la implementación de un sistema de honeypot Cowrie en Microsoft Azure, integrado con Microsoft Sentinel para la detección proactiva de amenazas. Ante la limitada visibilidad de los Centros de Operaciones de Seguridad (SOC) tradicionales, este proyecto propone una arquitectura de defensa que correlaciona eventos del honeypot con inteligencia de amenazas para identificar patrones de ataque en tiempo real, superando así la reactividad convencional.

El proyecto surge de la necesidad de anticiparse a intrusiones en entornos en la nube, estableciendo como objetivo principal el fortalecimiento de la detección temprana mediante el análisis avanzado de eventos. Fundamentado en la tríada CIA, el papel del SOC moderno y las capacidades de Microsoft Sentinel como SIEM nativo, el estudio emplea el lenguaje KQL para el procesamiento de datos y utiliza el marco MITRE ATT&CK para mapear tácticas y técnicas de adversarios, lo cual optimiza la respuesta ante incidentes.

El desarrollo técnico comprendió la creación de un entorno en Azure con una máquina virtual Ubuntu ejecutando Cowrie en contenedores Docker, configurando reglas de seguridad, la ingesta de logs vía Data Collection Rules hacia Log Analytics y la activación de inteligencia de amenazas. Tras el despliegue, se detectaron 707 direcciones IP únicas, permitiendo clasificar amenazas según su nivel de riesgo y confirmar tanto ataques conocidos como actividades maliciosas emergentes. El mapeo de los comandos más frecuentes, como la manipulación de archivos SSH o descargas de malware mediante utilidades estándar, validó la eficacia del honeypot en la identificación de tácticas, técnicas y procedimientos (TTPs)

reales, manteniendo un costo operativo estimado de 150 USD mensuales que asegura su viabilidad económica.

En conclusión, esta arquitectura demuestra ser tanto técnica como financieramente sostenible para mejorar la detección temprana en entornos empresariales. Se recomienda escalar el monitoreo hacia otros tipos de honeypots y avanzar en la automatización de respuestas mediante soluciones SOAR para maximizar la eficacia operativa del SOC frente a amenazas modernas.

Palabras Claves:

- **Seguridad en la nube:** Engloba el entorno de despliegue principal del proyecto.
- **Honeypot:** Identifica la herramienta de engaño utilizada para la captura de ataques.
- **Microsoft Sentinel:** Especifica la solución SIEM (Security Information and Event Management) empleada para la gestión de eventos.
- **Detección proactiva de amenazas:** Define el valor estratégico y el objetivo central de tu investigación.
- **Inteligencia de amenazas:** Hace referencia al uso de fuentes externas para correlacionar y dar contexto a los ataques capturados.
- **Marco MITRE ATT&CK:** Indica la metodología utilizada para mapear y clasificar el comportamiento de los atacantes.

ABSTRACT

This research addresses the implementation of a Cowrie honeypot system on Microsoft Azure, integrated with Microsoft Sentinel for proactive threat detection. Given the limited visibility of traditional Security Operations Centers (SOCs), this project proposes a defense architecture that correlates honeypot events with threat intelligence to identify attack patterns in real-time, thereby transcending conventional reactivity.

The project arises from the necessity to anticipate intrusions in cloud environments, establishing the primary objective of strengthening early detection through advanced event analysis. Grounded in the CIA triad, the role of the modern SOC, and the capabilities of Microsoft Sentinel as a cloud-native SIEM, the study employs KQL for data processing and utilizes the MITRE ATT&CK framework to map adversary tactics and techniques, which optimizes incident response.

The technical development involved creating an Azure environment with an Ubuntu virtual machine running Cowrie in Docker containers, configuring security rules, log ingestion via Data Collection Rules into Log Analytics, and activating threat intelligence. Following deployment, 707 unique IP addresses were detected, enabling threat classification by risk level and confirming both known attacks and emerging malicious activities. Mapping the most frequent commands, such as SSH file manipulation or malware downloads via standard utilities, validated the effectiveness of the honeypot in identifying real Tactics, Techniques, and Procedures (TTPs), while maintaining an estimated operating cost of 150 USD per month, ensuring economic viability.

In conclusion, this architecture proves to be both technically and financially sustainable for enhancing early detection in enterprise environments. It is recommended to

scale monitoring to other types of honeypots and advance response automation through SOAR solutions to maximize the SOC's operational effectiveness against modern threats.

Keywords:

- **Cloud Security**: Refers to the protection of cloud-based infrastructure and services, which serves as the primary environment for the project's deployment.
- **Honeypot**: Represents the deceptive technology used to lure, capture, and analyze malicious activity to improve security posture.
- **Microsoft Sentinel**: Identifies the cloud-native Security Information and Event Management (SIEM) solution used for advanced event correlation and security orchestration.
- **Proactive Threat Detection**: Highlights the strategic approach of identifying and mitigating threats before they cause damage, moving beyond traditional reactive methods.
- **Threat Intelligence**: Refers to the use of external data and context to identify and correlate attacks, providing deeper insights into malicious traffic.
- **MITRE ATT&CK Framework**: Defines the standardized knowledge base used to map and classify adversary tactics, techniques, and procedures (TTPs) observed during the research

ÍNDICE

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

CAPÍTULO 1

1. Introducción

El presente proyecto de investigación se enfoca en el diseño e implementación de un sistema de honeypot en la plataforma Microsoft Azure, utilizando el honeypot Cowrie como mecanismo de captura de actividad maliciosa en un entorno controlado. La solución contempla la exposición de servicios simulados a través de una máquina virtual con dirección IP pública y la habilitación de puertos específicos, con el propósito de emular un sistema vulnerable que permita atraer intentos reales de intrusión.

Los eventos generados por el honeypot serán recolectados, procesados e integrados en Microsoft Sentinel, donde se realizará la ingesta y correlación de datos mediante consultas en Kusto Query Language (KQL). Este enfoque permitirá transformar los registros capturados en información accionable, integrándolos con fuentes de inteligencia de amenazas propias del SIEM para identificar patrones, detectar comportamientos anómalos y fortalecer las capacidades de monitoreo.

La relevancia de esta investigación radica en la necesidad de adoptar enfoques proactivos en ciberseguridad, especialmente en entornos cloud, donde la superficie de ataque es cada vez más amplia y dinámica. A diferencia de los modelos tradicionales de detección, que dependen de eventos ya ocurridos, el uso de honeypots permite anticiparse a los ataques, capturando información directa sobre las tácticas y técnicas empleadas por los atacantes.

En este contexto, el proyecto propone no solo la implementación de un honeypot, sino su integración efectiva con un sistema SIEM que permita correlacionar los eventos generados con otras fuentes de datos, enriqueciendo la detección mediante inteligencia de amenazas. De esta manera, se busca demostrar cómo una arquitectura orientada a la detección temprana y la defensa proactiva puede mejorar significativamente la visibilidad y la capacidad de respuesta ante incidentes de seguridad.

1.1. Definición del proyecto

El proyecto consiste en la implementación de un sistema de Honeypot dentro de la plataforma Microsoft Azure para capturar y analizar actividades maliciosas en un entorno controlado, enviando estos registros a un Log Analytics Workspace para su integración en Microsoft Sentinel. La propuesta surge ante la limitación que muestran los SOC tradicionales, los cuales operan con una visibilidad limitada o carecen de inteligencia de amenazas lo cual hace que les cueste anticiparse ante ataques de forma proactiva. De acuerdo con los datos recopilados en la eS 2026 SOC Survey, realizada a 444 profesionales de operaciones del área seguridad se pudo identificar esta la falta de visibilidad a nivel empresarial como la principal barrera para la efectividad de un SOC, señalada por el 24% de los líderes de ciberseguridad (SANS Institute, 2026), a esto se adicionamos el carácter reactivo de estos centros: según (CyberDefenders, 2026) los analistas en los SOC suelen revisar un alto volumen de alertas con contexto limitado, dependiendo de indicadores externos en lugar de herramienta interna que permita anticipar amenazas.

En entornos Cloud, el valor diferencial de un Honeypot radica en su capacidad para actuar como un sensor avanzado que permite validar los tipos de ataques que se intentan perpetrar contra servicios expuestos a Internet, antes de que estos logren afectar los activos críticos, sin embargo, la brecha específica identificada es que el despliegue de un honeypot de forma aislada no garantiza la protección; es imperativo resolver la falta de correlación de estos eventos con los logs recopilados en el SIEM para generar reglas de detección efectivas ante patrones inusuales, es por ello que mediante el uso de consultas KQL y modelos de correlación, el sistema permitirá mapear técnicas de intrusión al framework MITRE ATT&CK y enriquecer los registros con feeds de inteligencia.

La correlación avanzada se ejecutará mediante el uso de reglas de analítica en el lenguaje KQL, que tendrán como fuente de inteligencia las IPs Origen, puertos, cantidad de

eventos y comandos ejecutados en periodos de tiempo que serán utilizados como condiciones para modelas reglas de Analítica programadas.

El trabajo busca demostrar cómo esta arquitectura fortalece la capacidad de monitoreo y respuesta ante incidentes, comparando la eficacia de un entorno convencional frente a uno robustecido mediante la integración proactiva de sistemas de detección; Para medir este impacto, se definirá como métrica la cantidad de eventos detectados, así como el volumen de direcciones IP y dominios maliciosos identificados durante el periodo de análisis, es decir, se realizará una comparación del número de IPs detectadas por el Honeypot únicamente, el número de IPs detectadas por la tabla de Microsoft únicamente y las IPs detectadas por ambas tablas, finalmente, se aplicará una asignación de puntaje del riesgo (Crítico, Alto, Medio, Bajo o Informativo) de la IP en base al comportamiento detectado calculado en función de si coincide con los indicadores de la tabla de Threat Intelligence de Microsoft y a la cantidad de comandos sospechosos ejecutados en el Honeypot, como por ejemplo intentos de descarga, escalamiento de privilegios o ejecución remota.

1.2. Justificación e importancia del trabajo de investigación

Ante la falta de visibilidad en los Centros de Operaciones de Seguridad y las amenazas cada vez más sofisticadas y dinámicas resulta imperativo adoptar un enfoque proactivo direccionado a identificar anomalías de forma temprana, con el fin de mitigar impactos considerables en la infraestructura o que se materialice un incidente de Seguridad.

Actualmente los SOC tradicionales cuentan con visibilidad limitada, ligada a las escasas herramientas y activos que se encuentran integradas, de hecho, la mayoría de ellos carecen de Inteligencia de amenazas o su integración tiene un costo considerable, por falta de un Honeypot que pueda capturar actividad maliciosa de manera controlada y así, anticiparse a un posible ataque, en entornos Cloud más específicamente el valor de tener un Honeypot se relaciona con la anticipación de validar que tipos de ataques se están intentando perpetrar en

servicios expuestos a Internet. Por otro lado, el simple hecho de levantar un Honeypot no resuelve el problema, es de vital importancia correlacionar estos eventos con los logs recopilados en el SIEM y crear reglas de detección efectivas que puedan detectar patrones inusuales de manera oportuna.

La integración de eventos generados mediante un honeypot a un SIEM aporta una amplia fuente de información a los Equipos de Inteligencia de Amenazas respecto a los grupos atacantes, Indicadores de Compromiso (IOCs), tales como ips o dominios utilizados por grupos APT (Amenazas Persistentes Avanzadas); así como, técnicas destinadas a escanear e intentar perpetrar posibles ataques. Por otro lado, mediante la integración de estas fuentes de inteligencias a un SIEM se facilita la cacería de amenazas basada en la infraestructura actual. Esto, sumado a un plan de respuesta a incidentes alineado a los marcos de referencia como la ISO/IEC 27035, garantiza una correcta respuesta frente a posibles ciberataques.

Utilizando un Honeypot de Cowrie, el cual requiere menores recursos de la máquina virtual y menores costos mensuales de despliegue y mantenimiento en comparación con opciones como T-POT, el cual integra varios honeypot, para este escenario nos centraremos en colectar logs de SSH, telnet y ejecución de comandos dentro de la sesión simulada del Honeypot, de la misma forma el sistema operativo seleccionado para levantar el Cowrie será Ubuntu dadas sus bondades de compatibilidad, estabilidad y su facilidad de integración con el entorno de Azure.

Además, para fortalecer la validación del sistema propuesto, se contempla la ejecución de una campaña de ataque simulada y controlada contra el honeypot. Esta actividad permitirá observar el comportamiento del sistema ante tácticas reales de intrusión y, posteriormente, mapear las técnicas identificadas al framework MITRE ATT&CK. Con ello se busca evaluar la capacidad del honeypot y de Microsoft Sentinel para detectar, clasificar y correlacionar actividades maliciosas alineadas a estándares internacionales de ciberseguridad.

El aporte fundamental de este trabajo es la creación de una Arquitectura de Defensa Proactiva Replicable. A diferencia de una implementación simple, este proyecto de tesis entregará un modelo de configuración de seguridad (Hardening) y un repositorio de reglas de detección (Detección como código) que las organizaciones pueden adoptar para robustecer sus SOC actuales bajo un esquema de costos optimizado en Azure.

1.3. Alcance del estudio

- Se implementará un honeypot en entorno virtual controlado dentro de la nube de Microsoft Azure.
- Se simularán campañas de ataque dirigidas que incluyen: Escaneos con Nmap, Intentos de intrusión para la ejecución de comandos remotos en el servicio emulado de SSH.
- Se definirá un volumen estimado de generación de eventos de seguridad en conjunto con logs diarios. El volumen de datos se estimará mediante la exposición del honeypot a internet durante un periodo de 30 días, mismos que serán evaluados mediante conteos diarios utilizando lógica construida en consultas KQL.
- Para la evaluación de la efectividad de la solución, se establecerán métricas como:
- Realizar la integración en el entorno sin honeypot y con honeypot modificando las fuentes de Inteligencia asociadas a las reglas de analítica.
- Se realizará la ingesta y correlación de indicadores de compromiso (IOCs) provenientes del honeypot cowrie, integrándolos con feeds de inteligencia de amenazas (Microsoft Threat Intelligence), con el objetivo de enriquecer los

registros del SIEM y mejorar la precisión en la detección de eventos de seguridad.

- Se generarán alertas de seguridad mediante la implementación de reglas de analítica desarrolladas en lenguaje KQL.
- Se realizará un análisis de costos del entorno implementado en la nube de Azure, con el fin de evaluar la viabilidad económica de la solución.
- Se documentará el proceso de implementación y configuración del escenario de pruebas el cual contiene Microsoft Sentinel, donde se almacenan las consultas KQL, las reglas NSG configuradas, los resultados obtenidos y una maquina en Azure donde se desplegó el Honeypot.

1.4. Objetivos

1.4.1 Objetivo general

Implementar un honeypot Cowrie en Microsoft Azure e integrar sus eventos con Microsoft Sentinel para mejorar la visibilidad de amenazas y la detección temprana de ciberataques mediante técnicas de correlación y análisis de eventos, comparando los resultados obtenidos con las fuentes de inteligencia de amenazas de Microsoft.

1.4.2. Objetivo específico

- Diseñar un entorno seguro y controlado en Microsoft Azure para el despliegue del honeypot.
- Integrar los registros generados por el honeypot con un Log Analytics Workspace y habilitar Microsoft Sentinel.
- Desarrollar un listado de reglas de analítica que permitan identificar intentos de intrusión basados en los resultados del Honeypot por periodos específicos de

tiempo.

- Analizar los eventos capturados para identificar comportamientos maliciosos y clasificar tácticas y técnicas utilizadas por atacantes.
- Realizar una evaluación comparativa entre un entorno sin honeypot y otro con honeypot, enfocándose en la fiabilidad de las ips comparándolas en diversas herramientas como virus total.
- Obtener un listado de comandos ejecutados desde dichas ips con el fin de evidenciar el aporte del sistema propuesto en la detección de actividades maliciosas.

CAPÍTULO 2

2. Revisión de literatura

2.1. Estado del arte

La evolución de las plataformas de Gestión de eventos e información de Seguridad (SIEM) hacia arquitecturas cloud-native ha transformado la detección de amenazas al mejorar significativamente la escalabilidad, la correlación y la eficiencia de costos. La eficacia de soluciones como Microsoft Sentinel reside en su capacidad para aplicar analítica avanzada sobre volúmenes masivos de datos, optimizando las operaciones en entornos híbridos y de nube (Sikos, L. F., 2023). Estudios independientes, como el análisis de Impacto Económico Total (TEI) realizado por Forrester (2024), cuantifican este avance: las instituciones que implementan Microsoft Sentinel reportan un retorno de inversión del 234% en tres años, una reducción del 79% en falsos positivos mediante analítica de comportamiento y una disminución del 93% en el tiempo de despliegue de nuevas conexiones. Además, la arquitectura de observabilidad nativa permite gestionar la complejidad de entornos multi-nube con mayor precisión (Al-Rubaian, A., & Al-Turjman, F., 2025)

Más allá de la centralización de registros, Sentinel actúa como una plataforma de Orquestación, Automatización y Respuesta (SOAR), facilitando la ejecución de playbooks que reducen la carga operativa ante incidentes complejos (Microsoft, 2024). Este nivel de automatización es respaldado por enfoques que integran la respuesta activa dentro de las operaciones del SOC, permitiendo que la respuesta sea tan rápida como la detección (Patel, K., & Gupta, M. , 2024).

En el ámbito de la defensa activa, el despliegue de sistemas de engaño (honeypots) en la nube ha emergido como una estrategia vital para obtener inteligencia contextualizada. Investigaciones recientes subrayan que la integración de estos sistemas con plataformas SIEM

permite a los equipos analizar vectores de ataque en tiempo real, superando las limitaciones de los sistemas de defensa pasivos (Varghese, S., et al., 2024). Dentro de este ecosistema, herramientas como Cowrie se han consolidado por su capacidad para emular servicios vulnerables (SSH/Telnet), capturando no solo el tráfico de fuerza bruta, sino el comportamiento del atacante tras la intrusión (D'souza, E., 2023). La eficacia de estos honeypots se ve potenciada cuando se despliegan mediante estrategias estandarizadas en entornos virtualizados, lo que garantiza su escalabilidad (Sánchez-Gómez, J., et al. , 2024).

La integración técnica entre Cowrie y Microsoft Sentinel representa un avance significativo: la ingesta de registros hacia el SIEM, procesada mediante consultas KQL, transforma datos brutos en alertas accionables. Esta sinergia facilita el mapeo de tácticas al framework MITRE ATT&CK, permitiendo identificar patrones antes de que comprometan la infraestructura productiva (Husari, G., 2022). Este proceso se optimiza aún más gracias a la analítica de comportamiento avanzada, que mejora la precisión en la caza de amenazas (threat hunting) (Zhang, Y., & Liu, H. , 2025).

Finalmente, la literatura actual enfatiza que el modelo de "Detección como Código" y el uso de listas de vigilancia (watchlists) son pilares fundamentales en un SOC moderno. La capacidad de Sentinel para correlacionar eventos de honeypots con inteligencia externa permite una reducción drástica en el Tiempo Medio de Detección (MTTD) y el Tiempo Medio de Respuesta (MTTR) (Al-Zewairi, M., 2022). La estandarización de estos procesos bajo el paradigma de "Detección como Código" se ha convertido en la norma para garantizar una postura de seguridad robusta y reproducible en entornos híbridos (Chen, X., & Wang, J. , 2026).

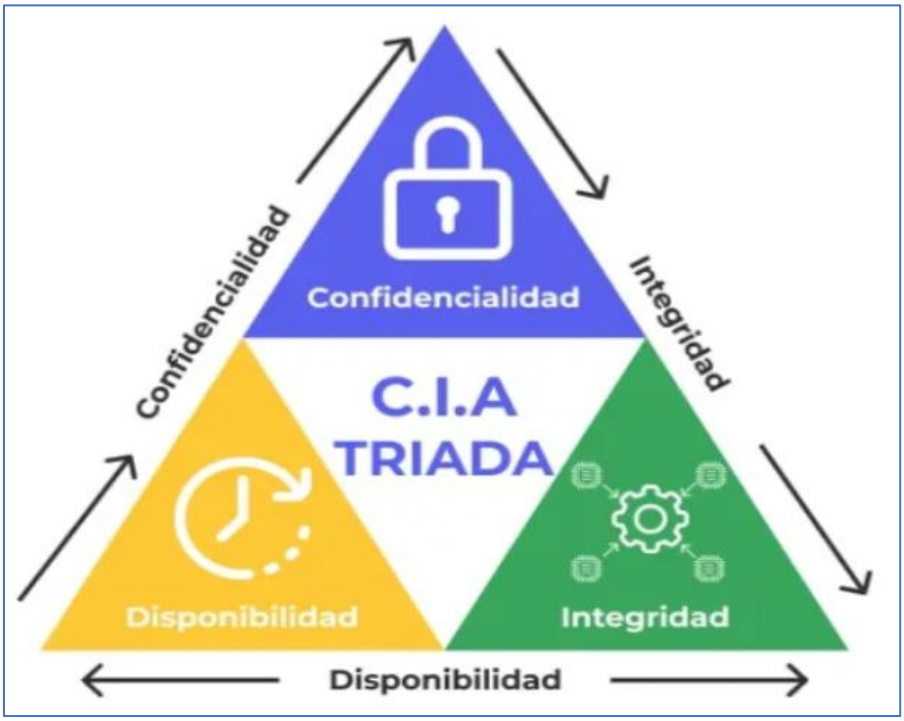
2.2. Marco teórico

2.2.1. Seguridad de la Información y Detección de Incidentes

La seguridad de la información se fundamenta en la protección de los activos tecnológicos y de información de una organización mediante los principios de confidencialidad, integridad y disponibilidad (CIA).

Figura 1.

Modelo CIA



Nota.: Adaptado de *Definición de la tríada de la CIA: ejemplos de confidencialidad, integridad y disponibilidad*, por Wallarm, 2026 (https://lab.wallarm.com/what/definicion-de-la-triada-de-la-cia-ejemplos-de-confidencialidad-integridad-y-disponibilidad/?lang=es).

Estos principios constituyen la base para el diseño e implementación de controles técnicos y organizacionales orientados a mitigar riesgos y reducir la probabilidad de impacto frente a eventos de seguridad.

Las normas internacionales ISO/IEC 27001 e ISO/IEC 27035 establecen un marco estructurado para la gestión de la seguridad de la información y la respuesta a incidentes, en conjunto con herramientas como un SIEM se logra soportar los requisitos establecidos, promoviendo la identificación temprana de amenazas, la contención oportuna y la recuperación controlada ante eventos de ciberseguridad. (Schim, 2023)

En entornos modernos, caracterizados por infraestructuras distribuidas y servicios expuestos a Internet, la detección reactiva resulta insuficiente. Por tal motivo, se han adoptado enfoques proactivos basados en monitoreo continuo, correlación y análisis contextual de eventos, los cuales permiten anticiparse a posibles amenazas y reducir el tiempo medio de detección (MTTD). (Torq, 2025)

2.2.2. Centro de Operaciones de Seguridad (SOC)

El Centro de Operaciones de Seguridad (SOC), es un equipo encargado del monitoreo continuo, análisis, detección y respuesta ante eventos de seguridad que afectan a una organización. Su función principal consiste en centralizar la visibilidad de los activos tecnológicos, analizar grandes volúmenes de datos y coordinar acciones de respuesta ante incidentes. (Microsoft, 2026)

Un SOC moderno integra múltiples fuentes de información, como dispositivos de red, endpoints, servicios en la nube y aplicaciones críticas. Generan eventos que, al ser analizados de manera aislada, pueden carecer de contexto suficiente; sin embargo, mediante técnicas de correlación y análisis centralizado, es posible identificar patrones complejos de ataque. (Microsoft, 2026)

En entornos cloud, los SOC han evolucionado hacia modelos híbridos o completamente basados en la nube, apoyándose en plataformas SIEM nativas que ofrecen escalabilidad, alta disponibilidad y capacidades avanzadas de análisis. La incorporación de mecanismos activos de detección, como los honeypots, permite ampliar la superficie de visibilidad y obtener información directa sobre intentos reales de ataque contra la infraestructura.

2.2.3. Sistemas de Gestión de Información y Eventos de Seguridad (SIEM)

Un Sistema de Gestión de Información y Eventos de Seguridad (SIEM), es una solución encargada de recopilar, normalizar, almacenar y analizar eventos de seguridad provenientes de múltiples fuentes dentro de una infraestructura tecnológica. Su principal objetivo es proporcionar una visión centralizada del estado de seguridad del entorno y facilitar la detección de amenazas mediante análisis y correlación de eventos. (Microsoft, 2026)

Los SIEM recopilan logs de dispositivos de red, sistemas operativos, aplicaciones, servicios cloud y soluciones de seguridad, permitiendo identificar comportamientos anómalos que podrían pasar desapercibidos de forma individual. Entre sus funcionalidades principales se incluyen la correlación de eventos, generación de alertas, visualización mediante dashboards y soporte para análisis forense.

2.2.4. Honeypots como mecanismos de detección proactiva

Un honeypot es un sistema o servicio diseñado intencionalmente para simular vulnerabilidades o activos legítimos con el objetivo de atraer, detectar y analizar actividades maliciosas. A diferencia de los sistemas tradicionales de protección, los honeypots no buscan prevenir ataques, sino observar el comportamiento del atacante y recopilar información valiosa sobre técnicas, herramientas y patrones utilizados. (Fortinet, 2026).

En la era de la arquitectura Zero Trust, los honeypots han evolucionado para dejar de ser componentes aislados y convertirse en herramientas de detección de alta fidelidad. Estudios recientes destacan que el despliegue de honeypots en la periferia de la red cloud reduce significativamente el tiempo de detección de intrusos (MTTD), al proporcionar señales de alerta temprana basadas en interacciones no autorizadas con activos falsos. (CISA., 2025)

Los honeypots se clasifican comúnmente según su nivel de interacción:

- Baja interacción, que simulan servicios básicos y reducen el riesgo operativo.
- Media interacción, que permiten una interacción limitada.
- Alta interacción, que replican entornos reales con mayor nivel de detalle.

En entornos cloud, los honeypots actúan como sensores avanzados, proporcionando visibilidad directa sobre escaneos, intentos de acceso no autorizado, explotación de servicios y abuso de credenciales. Sin embargo, su verdadero valor se alcanza cuando los eventos generados son correlacionados con otros registros de seguridad dentro de un SIEM, permitiendo contextualizar las amenazas observadas.

Para este proyecto se utiliza Cowrie, un honeypot de media interacción especializado en la simulación de servicios SSH y Telnet, ampliamente adoptado por la comunidad debido a su facilidad de implementación, bajo costo y capacidad de registrar comandos, credenciales y comportamientos maliciosos, mismos que pueden ser capturados y normalizados en el SIEM de Microsoft Sentinel (Warren Z. Cabral, 2022)

2.2.5. Correlación de eventos y análisis mediante KQL

La correlación de eventos consiste en analizar múltiples registros de seguridad de forma conjunta con el fin de identificar relaciones temporales, lógicas o contextuales que indiquen una actividad maliciosa. Esta técnica permite transformar eventos aislados en incidentes significativos, facilitando su análisis y respuesta.

Microsoft Sentinel utiliza Kusto Query Language (KQL) como lenguaje principal para la consulta y análisis de datos. KQL permite aplicar filtros, agregaciones, funciones estadísticas y enriquecimiento de datos, posibilitando la detección de patrones complejos de ataque. (Microsoft , 2026)

Mediante la correlación de eventos provenientes de honeypots con otros logs del entorno como autenticaciones, tráfico de red o actividad en máquinas virtuales es posible identificar fases completas del ataque, desde el reconocimiento inicial hasta intentos de persistencia o evasión de defensas.

2.2.6. Marco MITRE ATT&CK

El framework MITRE ATT&CK es una base de conocimiento que documenta tácticas, técnicas y procedimientos (TTPs) utilizados por actores maliciosos en ataques reales. Este marco permite categorizar y entender el comportamiento del adversario a lo largo del ciclo de ataque. (IBM , 2026)

Microsoft Sentinel incorpora de forma nativa el mapeo de detecciones al marco MITRE ATT&CK, facilitando la clasificación de eventos según tácticas como Reconocimiento, Acceso Inicial, Ejecución, Persistencia, Evasión de Defensa y Comando y Control. Este enfoque estandarizado mejora la comprensión del incidente y permite priorizar acciones de respuesta en función de la fase del ataque.

En el contexto de este proyecto, las técnicas observadas a través del honeypot son mapeadas al framework MITRE ATT&CK, permitiendo evaluar el nivel de exposición del entorno y la efectividad del sistema de detección implementado. Existen 14 tácticas, 216 técnicas y 475 sub-tecnicas que cubren las amenazas que se pueden utilizar por un ciberdelincuente para perpetrar un ataque, además de estas técnicas este framework incluye información de campañas y Grupos APT. (MITRE Corporation , 2025)

Figura 2.

Matriz MITRE

***Nota.*:** Adaptado de *MITRE ATT&CK® Enterprise Matrix*, por MITRE Corporation, s.f. (https://attack.mitre.org/matrices/enterprise/).

2.2.7. Inteligencia de Amenazas

La Inteligencia de Amenazas (Cyber Threat Intelligence – CTI) se define como el conocimiento basado en evidencia sobre amenazas actuales o potenciales, incluyendo indicadores de compromiso (IoCs), tácticas, técnicas, procedimientos y motivaciones de los atacantes. La CTI se clasifica comúnmente en niveles estratégico, táctico y operativo. (Microsoft, 2026).

La automatización del ciclo de vida de la Inteligencia de Amenazas, mediante el uso de protocolos estandarizados, es hoy un requerimiento mandatorio para cualquier centro de operaciones. La integración de fuentes dentro de ecosistemas cloud permite el enriquecimiento automático de los registros de auditoría, transformando indicadores brutos (como direcciones IP maliciosas) en contextos de ataque accionables que permiten una respuesta proactiva ante campañas de malware emergentes. (OASIS Open , 2024)

2.2.7.1. Inteligencia de Amenazas Táctica.

Permite a los centros de operaciones de seguridad (SOC) anticiparse ante futuros ataques y optimizar la detección de incidentes en curso. Además, es ideal para rastrear amenazas persistentes avanzadas (APT) y otros atacantes maliciosos que actúan de forma encubierta.

2.2.7.2. Inteligencia de Amenazas Operativa.

Este tipo de inteligencia tiene como objetivo brindar información que aporte en la toma de decisiones, mediante la identificación de actores de amenazas que pueden atacar a organizaciones y definir la estrategia más efectiva para hacerle frente a los ataques.

2.2.7.3. Inteligencia de Amenazas Estratégica.

Otorga una visión minuciosa ante las amenazas cibernéticas que afrontan las organizaciones permitiendo alinear inversiones y estrategias de gestión de riesgos ante una perspectiva de seguridad digital.

Microsoft Sentinel permite la integración de inteligencia de amenazas mediante Microsoft Threat Intelligence, enriqueciendo los eventos con información sobre la reputación de direcciones IP, dominios y otros indicadores. Esta integración mejora la capacidad de detección, reduce falsos positivos y facilita la priorización de alertas relevantes.

La combinación de honeypots con inteligencia de amenazas proporciona una visión enriquecida del panorama de amenazas, permitiendo no solo detectar ataques, sino también comprender su origen, intención y posibles impactos. Este enfoque fortalece significativamente la detección temprana y proactiva de eventos de seguridad en entornos cloud.

2.2.8. Indicadores de Compromiso (IOCs)

Datos que identifican cuando un sistema pudo haber sido atacado por una amenaza cibernética y a su vez, responde de manera eficaz ante dichos ataques. Además, ofrecen

información clave a los equipos especializados para analizar causas e incidencia tras una brecha o violación de red de seguridad. (SentinelOne, 2025).

2.2.9. Estándares STIX/TAXII

Structured Threat Information eXpression es una iniciativa global para impulsar la comunicación de información sobre amenazas y a su vez, la colaboración entre plataformas y organizaciones. (Cloudflare, 2026)

Si bien STIX define la estructura de la información de amenazas, es necesario incorporar el concepto de TAXII (Trusted Automated eXchange of Indicator Information), el cual corresponde a un protocolo diseñado para el intercambio automatizado de dicha información entre plataformas y organizaciones. En este contexto, TAXII permite la distribución de indicadores de compromiso (IoC) y datos de inteligencia en formato STIX de manera estandarizada.

En relación con Microsoft Sentinel, TAXII tiene un rol fundamental, ya que posibilita la ingesta automatizada de inteligencia de amenazas desde fuentes externas (feeds), permitiendo que estos indicadores sean utilizados en la correlación de eventos, generación de alertas y mejora en la detección de actividades maliciosas dentro del entorno monitoreado.

2.2.1 Honeypot de Cowrie

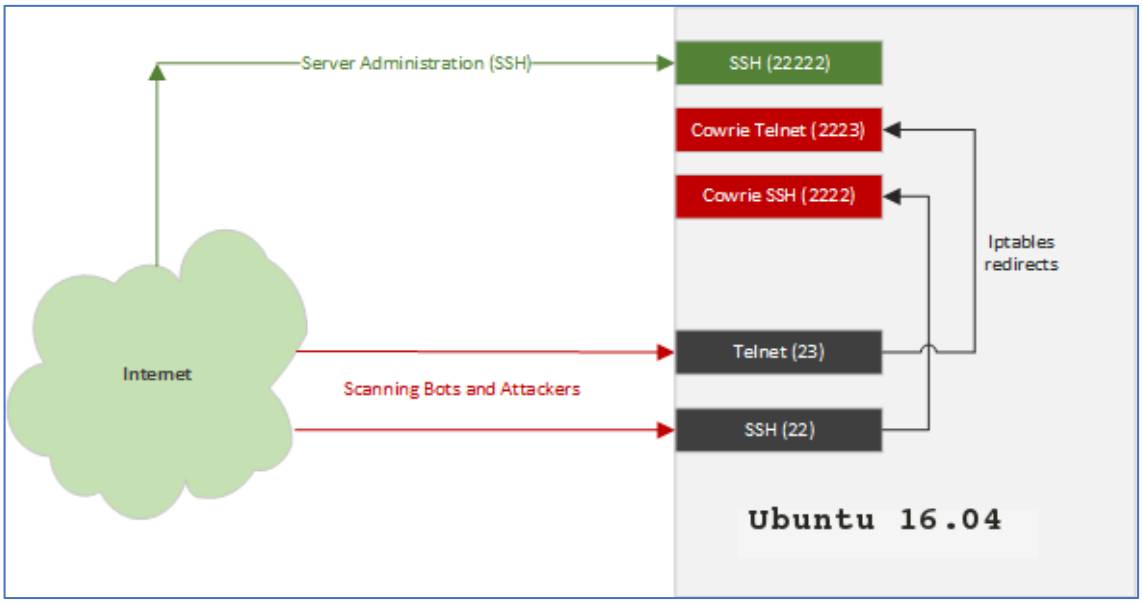
Se trata de un Honeypot con interacción entre media (emula un sistema UNIX en Python) y alta (Simula un proxy SSH) que simula servicios de SSH y Telnet vulnerables es una herramienta ideal para la detección de amenazas, recogida de malware y el análisis de los ataques, brindando inteligencia de amenazas e integración con herramientas SIEM. (Cowrie, 2024).

Se trata de un Honeypot con interacción entre media (emula un sistema UNIX en Python) y alta (Simula un proxy SSH) que simula servicios de SSH y Telnet vulnerables es una herramienta ideal para la detección de amenazas, recogida de malware y el análisis de los

ataques, brindando inteligencia de amenazas e integración con herramientas SIEM. (Cowrie, 2024). En este proyecto, Cowrie será tratado como un honeypot de media interacción, debido a que simula servicios SSH y Telnet en un entorno controlado, permitiendo la recolección de eventos e indicadores de ataque sin comprometer un sistema real.

Figura 3.

Arquitectura de Honeypot Cowrie



***Nota.*:** Adaptado de *Install Cowrie Honeypot on Ubuntu*, por HackerTarget, 2018 (https://hackertarget.com/cowrie-honeypot-ubuntu/).

2.2.2 Arquitectura de un Sistema de Honeypots Integrado con SIEM

Los honeypots modernos forman parte de arquitecturas de seguridad integradas que incluyen mecanismos de monitoreo, análisis y despliegue en entornos cloud. (D, 2023)

Esta arquitectura generalmente incluye:

- **Sensores (honeypots):** Capturan eventos maliciosos.

- **Recolección de logs:** Almacenamiento centralizado.
- **SIEM:** Análisis y correlación de eventos.
- **Inteligencia de amenazas:** Enriquecimiento de datos.

Figura 4.

Arquitectura de un Honeypot Integrado con SIEM

Nota.: El diagrama presentado fue generado con la asistencia de herramientas de inteligencia artificial para la estructuración gráfica, basándose en la configuración técnica diseñada por el autor.

Microsoft Sentinel actúa como núcleo de análisis, correlacionando eventos provenientes de Honeypots con otras fuentes de datos. Esta integración permite transformar datos aislados en información procesable, facilitando la detección de ataques complejos y coordinados. (Behl, 2017)

La eficacia de esta arquitectura radica en la calidad y el contexto de la telemetría recolectada. En entornos cloud, la integración profunda de los sensores (honeypots) con la capa

de ingesta del SIEM es fundamental para habilitar el análisis de comportamiento en tiempo real. Esta visibilidad permite que los registros de los señuelos no operen de forma aislada, sino que alimenten modelos de detección que permiten identificar patrones de movimiento lateral antes de que el atacante alcance activos de producción. (NIST , 2025)

2.2.3 Correlación de Eventos en Microsoft Sentinel para la Detección Proactiva

La correlación de eventos es un proceso esencial en los sistemas SIEM modernos, que permite identificar patrones complejos de ataque a partir de múltiples eventos aparentemente aislados. (Behl, 2017). En Microsoft Sentinel, esta correlación se realiza mediante reglas analíticas que integran datos provenientes de distintas fuentes, como:

- Honeypots de Cowrie desplegados en Azure. (Eventos de autenticación y ejecución de comandos)
- Threat Intelligence

La inclusión de Honeypots introduce un enfoque proactivo, ya que estos sistemas están diseñados para ser atacados y capturar comportamientos maliciosos reales. Al correlacionar estos eventos con inteligencia de amenazas y marcos como MITRE ATT&CK, es posible identificar tácticas, técnicas y procedimientos utilizados por los atacantes.

Ejemplos de actividades detectables incluyen:

- Intentos de acceso no autorizado a servicios expuestos.
- Escaneo de puertos y reconocimiento.
- Ejecución de comandos sospechosos en Honeypots.
- Transferencia de archivos maliciosos.

La correlación contextualizada permite identificar ataques avanzados que generan múltiples eventos distribuidos, mejorando la detección de amenazas persistentes y sofisticadas.

2.2.4 Reglas de Correlación en Microsoft Sentinel

Las reglas de correlación en Microsoft Sentinel permiten definir condiciones específicas bajo las cuales se genera una alerta de seguridad. Estas reglas pueden ser personalizadas o predefinidas, y se basan en consultas escritas en Kusto Query Language (KQL). (Microsoft, 2024)

La implementación de reglas de correlación efectivas trasciende la simple configuración de umbrales; implica la creación de una lógica que traduzca el comportamiento del atacante en incidentes de alta prioridad. Según las prácticas recomendadas por Microsoft, la estructuración de estas reglas mediante KQL permite no solo la detección estática, sino también el análisis del comportamiento anómalo basándose en la secuencia temporal de los eventos. Este enfoque es crucial para reducir la fatiga de alertas en los equipos de SOC, al garantizar que las notificaciones generadas estén alineadas directamente con tácticas reconocidas por marcos de referencia globales. (Microsoft , 2025)

A diferencia del enfoque basado en SPL de Splunk, KQL está optimizado para el análisis de grandes volúmenes de datos en entornos Cloud, permitiendo consultas rápidas y eficientes sobre datos almacenados en Azure. Las reglas de Analítica en Microsoft Sentinel permiten validar posibles eventos utilizando el lenguaje KQL, dentro de la configuración de las reglas de analítica es posible especificar la severidad, la descripción, las técnicas y tácticas de MITRE asociadas, la lógica KQL, el tiempo de ejecución y la asociación con algún Logic App para poder no solo generar un alertamiento hacia una posible alerta de seguridad sino también los procesos automatizados SOAR, es posible crear reglas de analítica partiendo de plantillas generadas y mantenidas por Microsoft o generar reglas de analítica “custom” especificando cada uno de los parámetros antes mencionados. (Microsoft, 2024)

Las reglas de correlación permiten:

- Detectar patrones de ataque en honeypots.

- Relacionar eventos de múltiples fuentes.
- Generar alertas automáticas ante comportamientos sospechosos.
- Activar playbooks de respuesta automatizada (SOAR).

La correcta configuración de estas reglas es clave para minimizar falsos positivos y maximizar la detección de amenazas relevantes. (Oprea, 2018)

2.2.5 Tácticas, técnicas y procedimientos (TTPs)

El análisis de TTPs permite comprender el comportamiento de los atacantes más allá de simples indicadores. Este enfoque está estructurado en marcos como MITRE ATT&CK. (MITRE, 2024)

Los honeypots son especialmente útiles para capturar TTPs en tiempo real, ya que permiten observar:

- Métodos de acceso inicial.
- Técnicas de escalamiento de privilegios.
- Movimientos laterales.
- Técnicas antiforenses. (Strom, 2018)

La correlación de estos datos en un SIEM facilita la identificación de ataques avanzados y persistentes.

CAPÍTULO 3

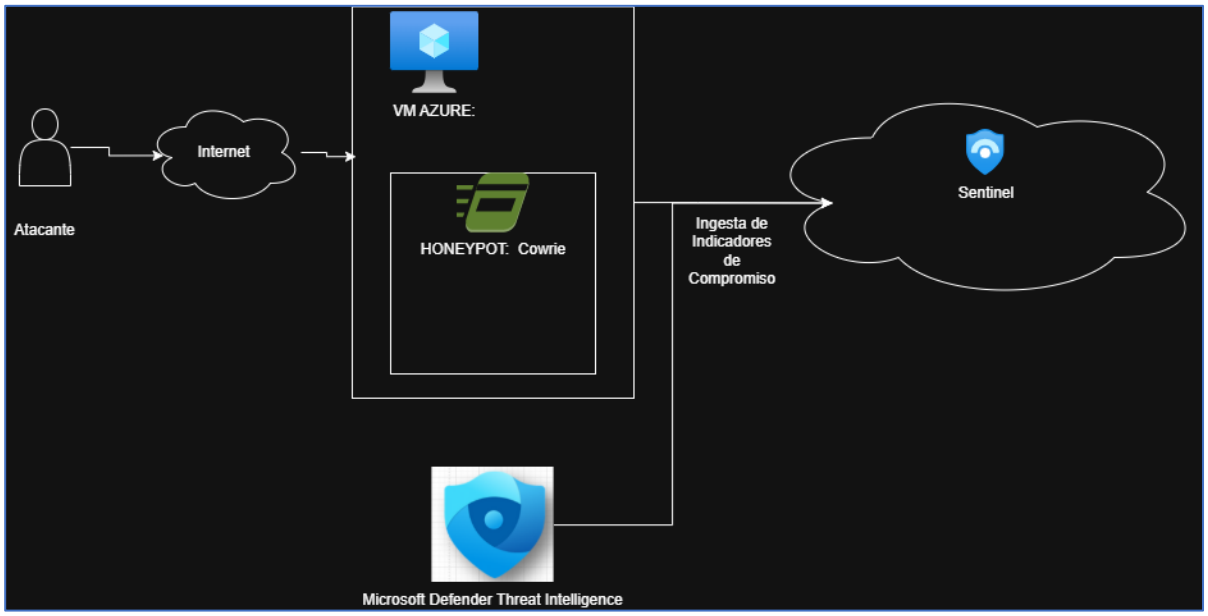
3. Desarrollo

3.1. Desarrollo del trabajo

Para el desarrollo del trabajo se explicará cómo se creó la cuenta de Azure, creación de suscripción, Log Analytic Workspace (En el que se alojara Microsoft Sentinel), Despliegue de Microsoft Sentinel, Creación de Máquina virtual con sistema operativo Linux Ubuntu, despliegue de Maquina Honeypot, Creación de Reglas NSG para acceso, Pruebas de acceso, Activación de conector para ingestar logs de Fuentes de Inteligencia de Microsoft, Creación de la Data Collection Rule (DCR) que nos permitirá enviar los logs de la maquina Ubuntu hacia el SIEM de Sentinel, Construcción de Consultas KQL para correlación y Resultados obtenidos, Mientras que al definir la arquitectura a alto nivel se tiene un sistema honeypot de cowrie levantado en una máquina de Azure el cual enviará logs simultaneamente con los indicadores de Microsft Defender Threat Intelligence hacia Microsoft Sentinel:

Figura 5.

Arquitectura de Honeypot en Azure



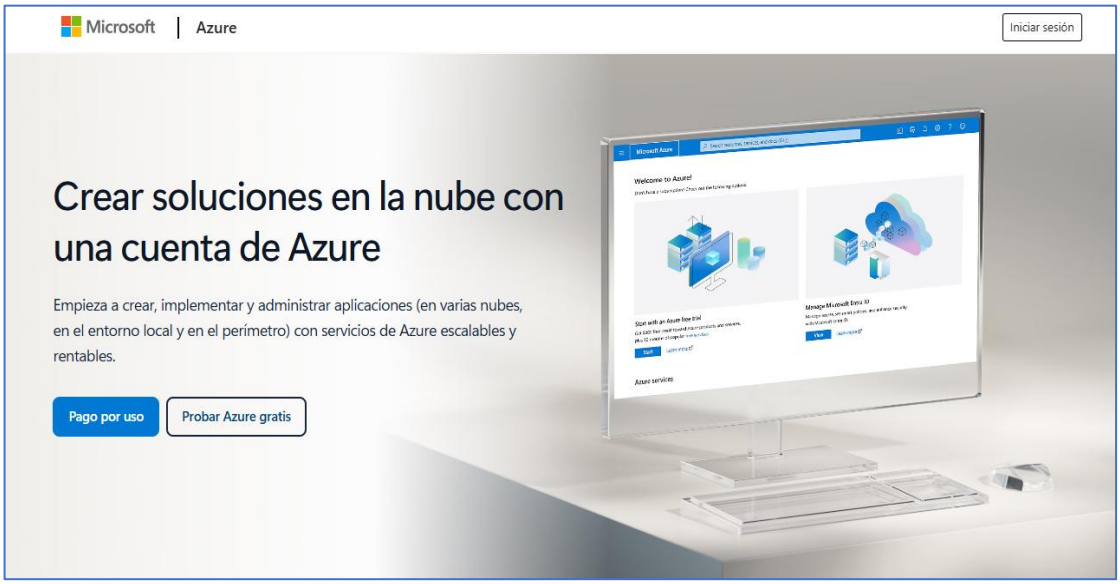
3.1.1 Suscripción Azure

- **Crear cuenta Azure**

En esta fase se realizó el registro en el portal de Microsoft Azure, con el objetivo de contar con una suscripción activa que permita desplegar y gestionar recursos en la nube para el laboratorio.

Figura 6.

Portal de Azure

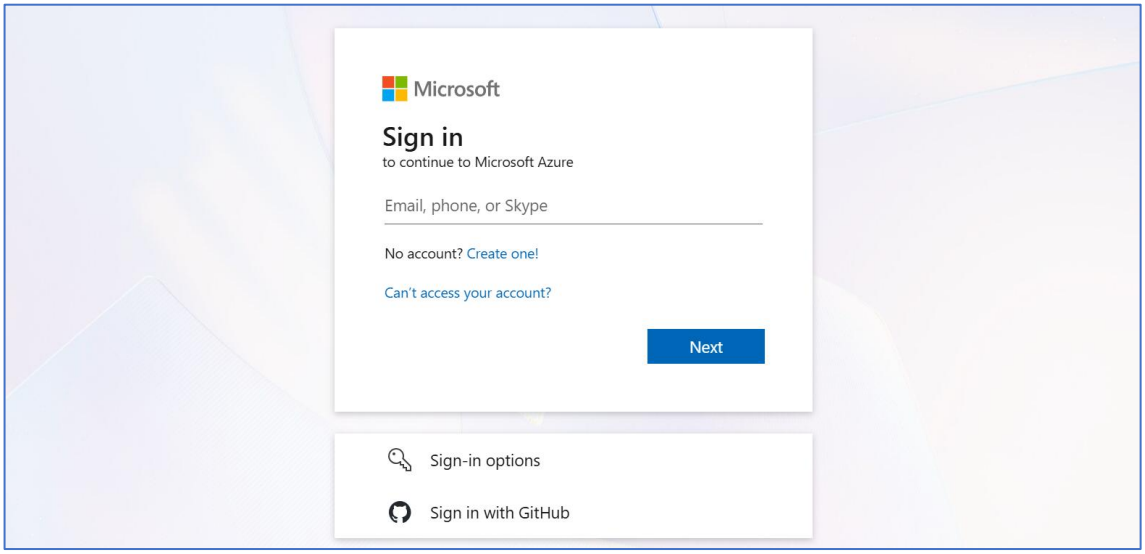


- **Portal de Azure / Inicio de sesión**

Se accedió al portal oficial de Microsoft Azure https://portal.azure.com, donde se inició sesión con una cuenta personal.

Figura 7.

Inicio de sesión

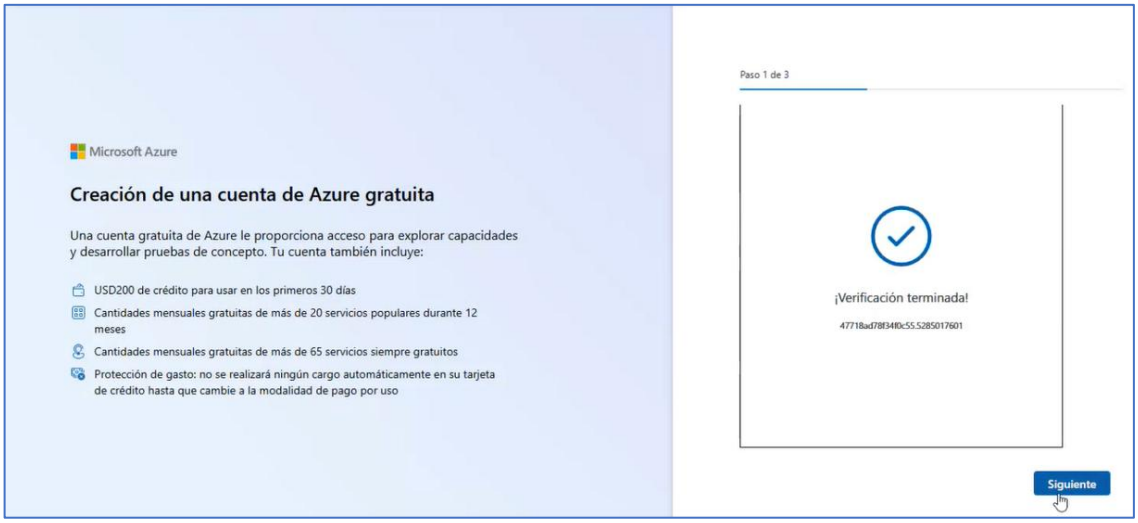


- **Activación de suscripción**

Se activó la suscripción de Azure, optando por el plan de prueba gratuita (Free Trial), el cual proporciona créditos iniciales para la creación y prueba de recursos sin costo.

Figura 8.

Activación de suscripción

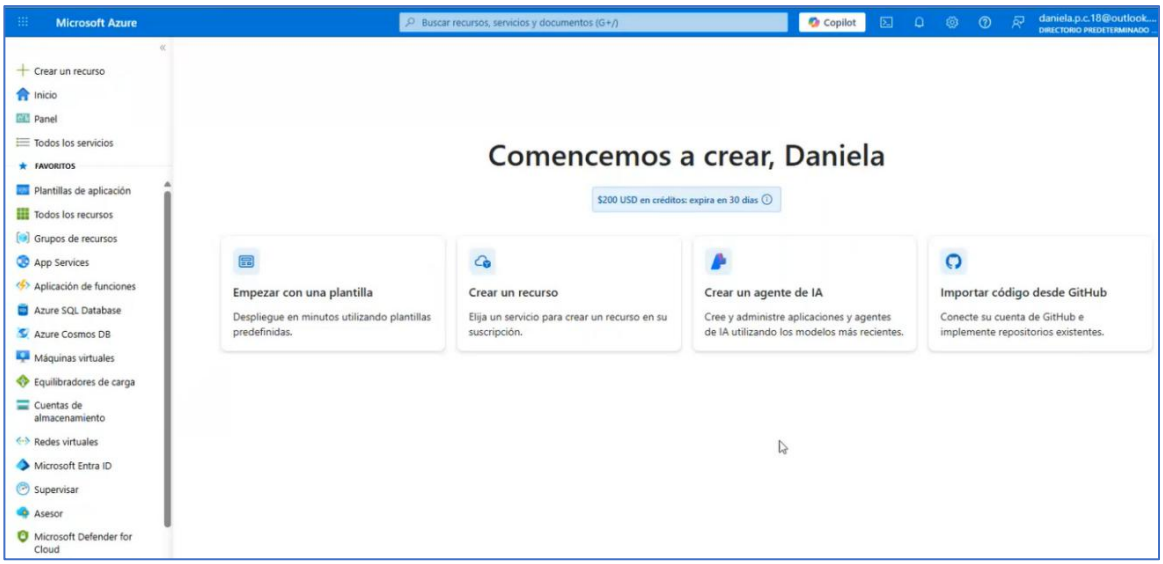


- **Portal inicial de Microsoft Azure**

Se evidencia que la suscripción de Microsoft Azure se encuentra correctamente habilitada y operativa para su uso. Además, se dispone de un crédito inicial de 200 USD correspondiente al plan de prueba gratuita, el cual permitirá desplegar y probar los recursos necesarios para el desarrollo del laboratorio.

Figura 9.

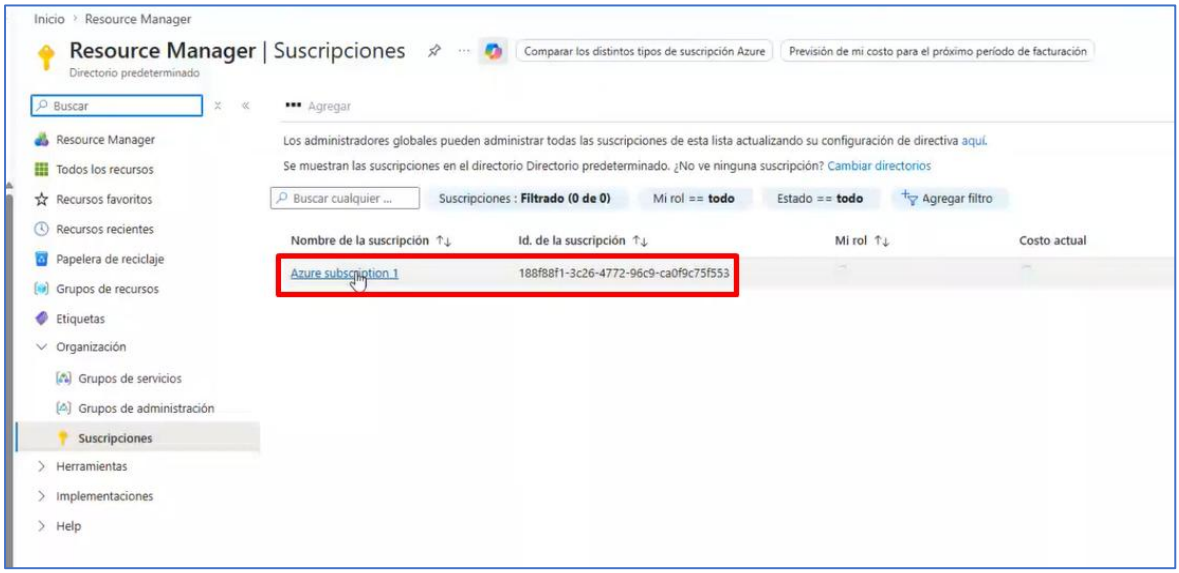
Dashboard Inicial de Azure



Una vez que contamos con la suscripción activa es posible validar en el Resource Manager el id de la suscripción:

Figura 10.

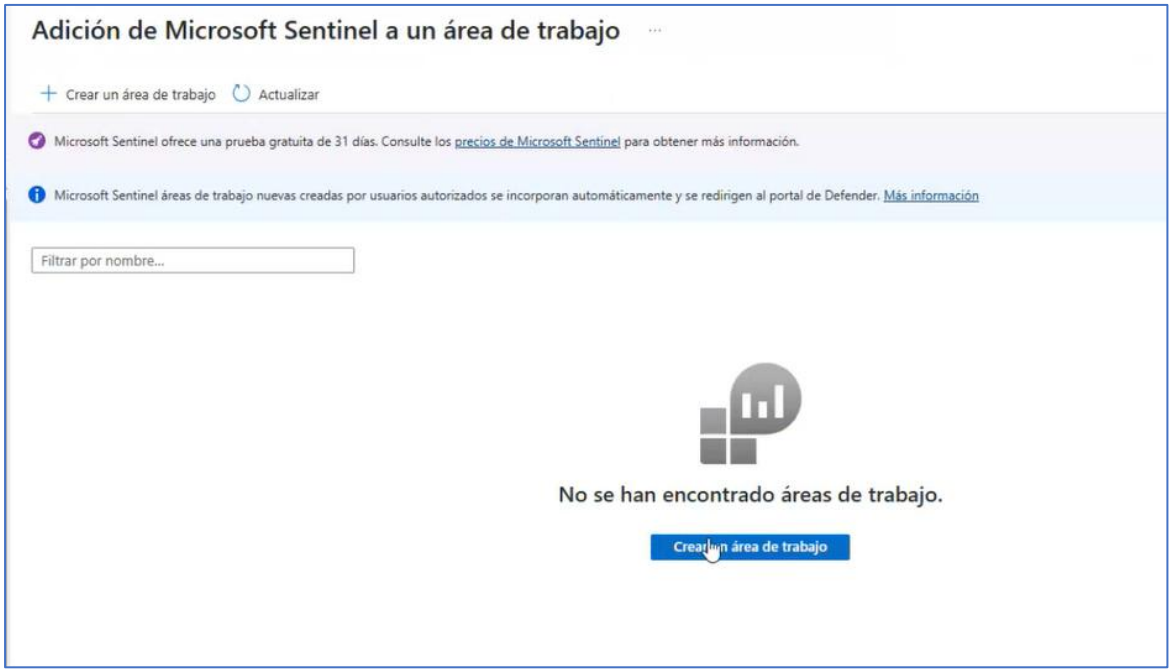
Suscripción activa en Resource Manager



Luego de tener la suscripción es posible crear un área de trabajo que alojara Microsoft Sentinel:

Figura 11.

Microsoft Sentinel - Area de trabajo



- **Creación de Area de Trabajo**

Es necesario definir una región, en este caso utilizaremos East US 2 (142,85$ mensual) dado que tiene menor latencia y costos reducidos dado que el laboratorio se realizó en Latinoamérica, las otras opciones comparadas fueron Brazil (227$ mensual), Chile (200,14$ mensual) y Mexico (156,98$ mensual), de donde East US 2 tuvo un menor costo y menor latencia que las demás opciones.

Figura 12.

Tabla de Latencia Microsoft

Norteamérica / Sudamérica | Europa | Asia-Pacífico (APAC) | Oriente Medio / África

Tablas de latencia para regiones de América, incluyendo EE. UU., Canadá y Brasil.

Utiliza las siguientes pestañas para ver las estadísticas de latencia de cada región.

Oeste de EE. UU. | Centro de EE. UU. | Este de EE. UU. | Canadá | Sudamérica

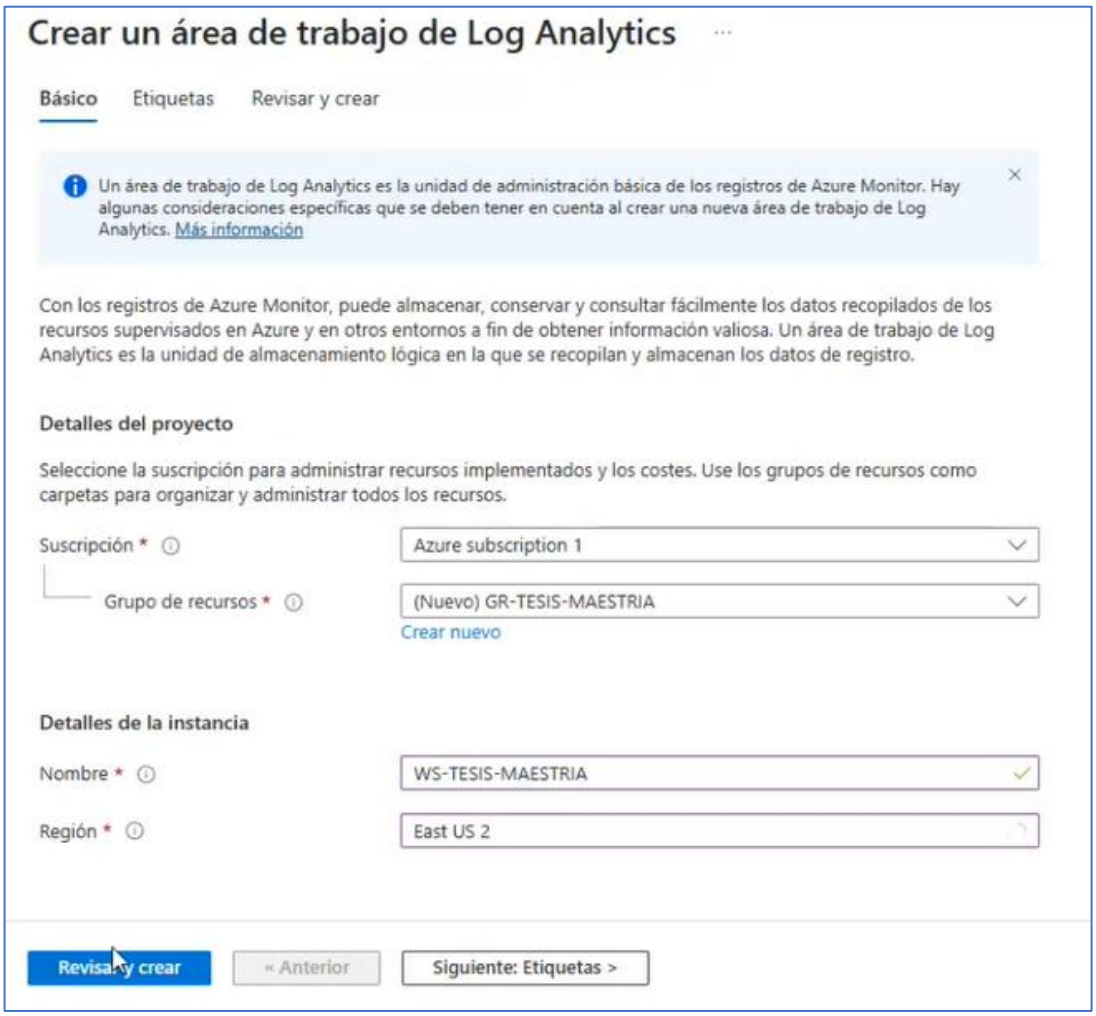
Expand table

Fuente	Brasil Sur	México Central
Australia Central	300	182
Australia Central 2	300	182
Australia Este	298	183
Australia Sureste	309	190
Brasil Sur		157
Canadá Central	132	70
Canadá Este	135	79
Central India	306	265
Centro de EE. UU.	149	45
Asia Oriental	314	189
Este de EE. UU.	121	56
East US 2	119	48

Indica que se colocó un valor referencial de la calculadora de Azure simulando los costos de la máquina virtual, además se creó un grupo de recursos llamado “GR-TESIS-MAESTRIA”, finalmente una instancia con nombre “WS-TESIS-MAESTRIA”:

Figura 13.

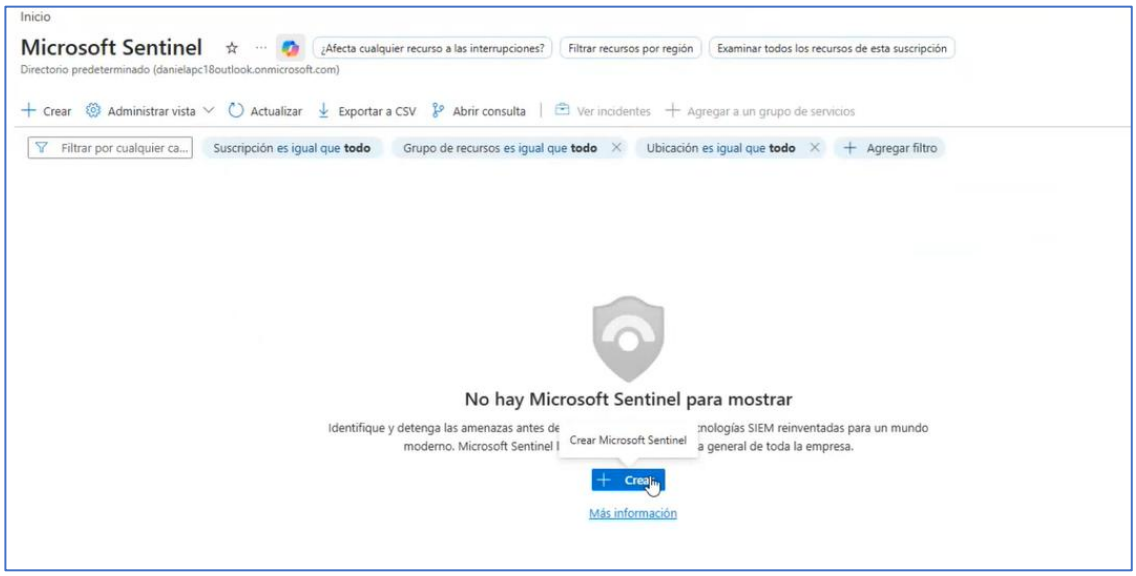
Creación del área de trabajo



Una vez creada el área de trabajo se procederá a levantar el SIEM de Microsoft Sentinel:

Figura 14.

Levantamiento del SIEM

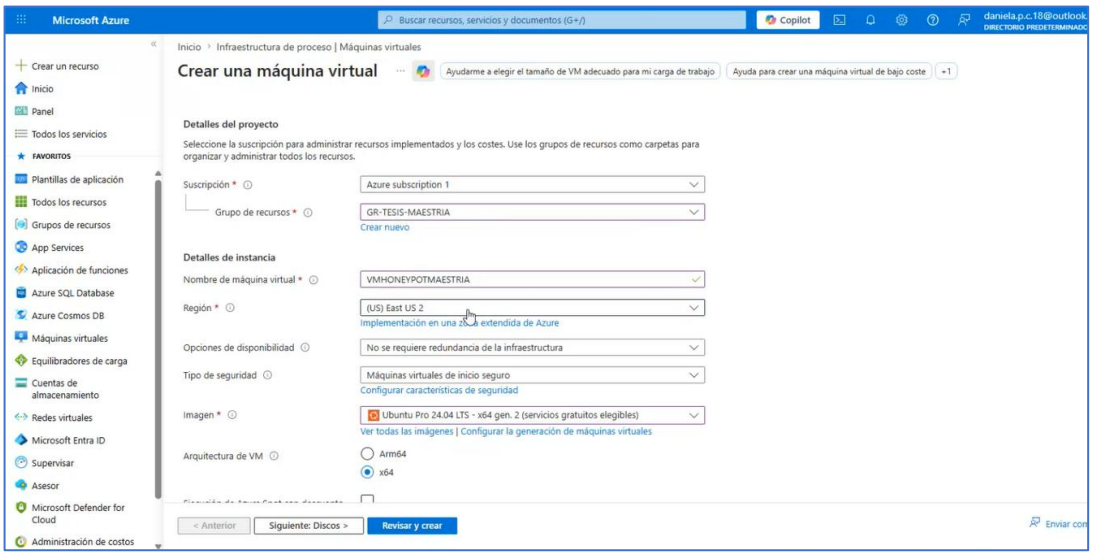


- **Creación de Máquina Virtual**

La máquina se asignó al grupo de recursos creado anteriormente, se definió el nombre de la máquina virtual, la imagen asociada, para este caso una imagen de Ubuntu Pro 24.04 LTS.

Figura 15.

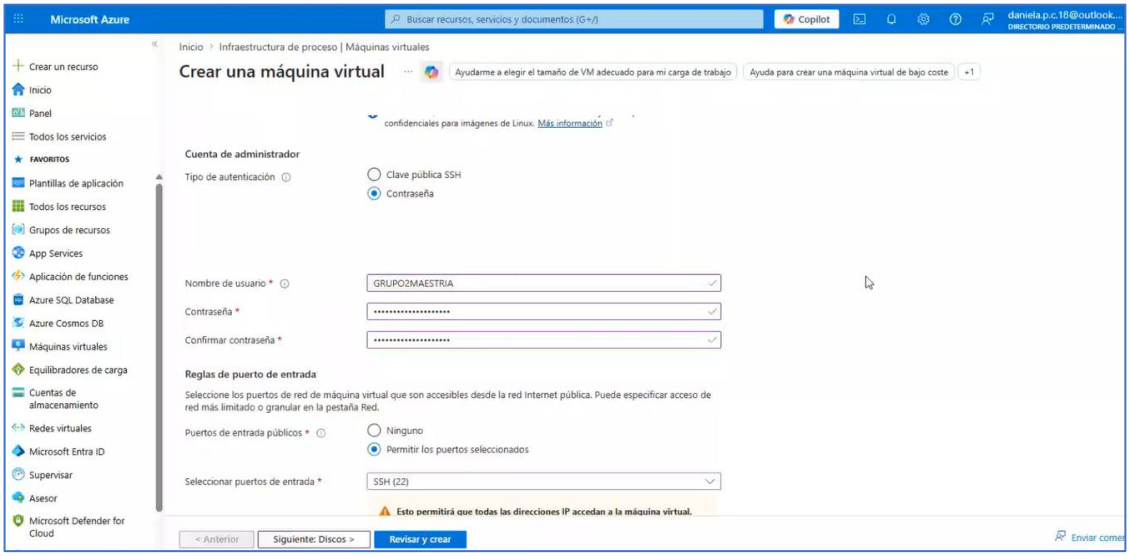
Creación de máquina virtual



Luego, se creó un usuario y contraseña para el acceso mediante SSH:

Figura 16.

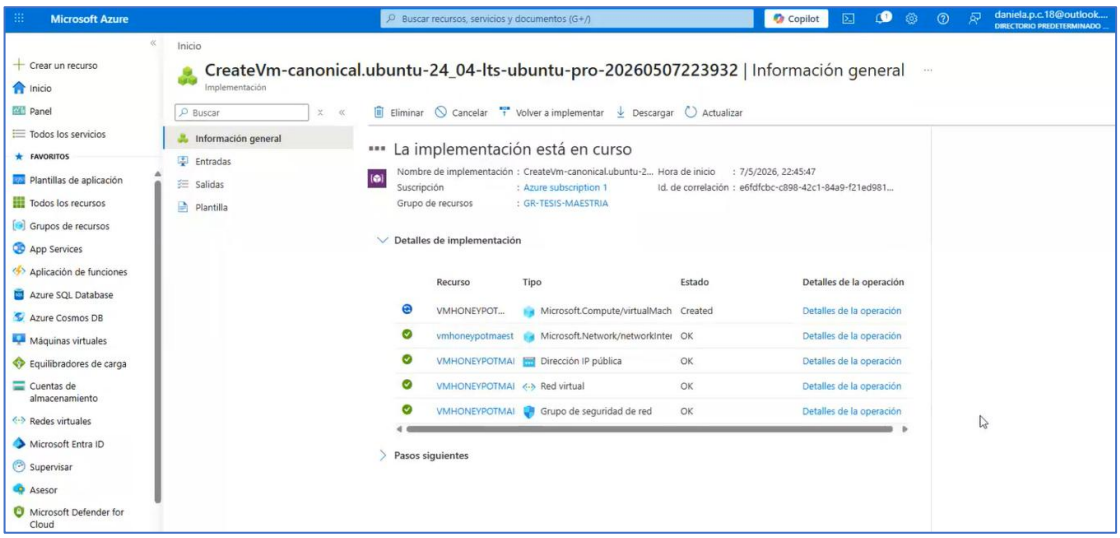
Avance de creación de máquina virtual



Luego de la configuración de la máquina se procedió al despliegue de los siguientes recursos:

Figura 17.

Listado de recursos en creación de VM



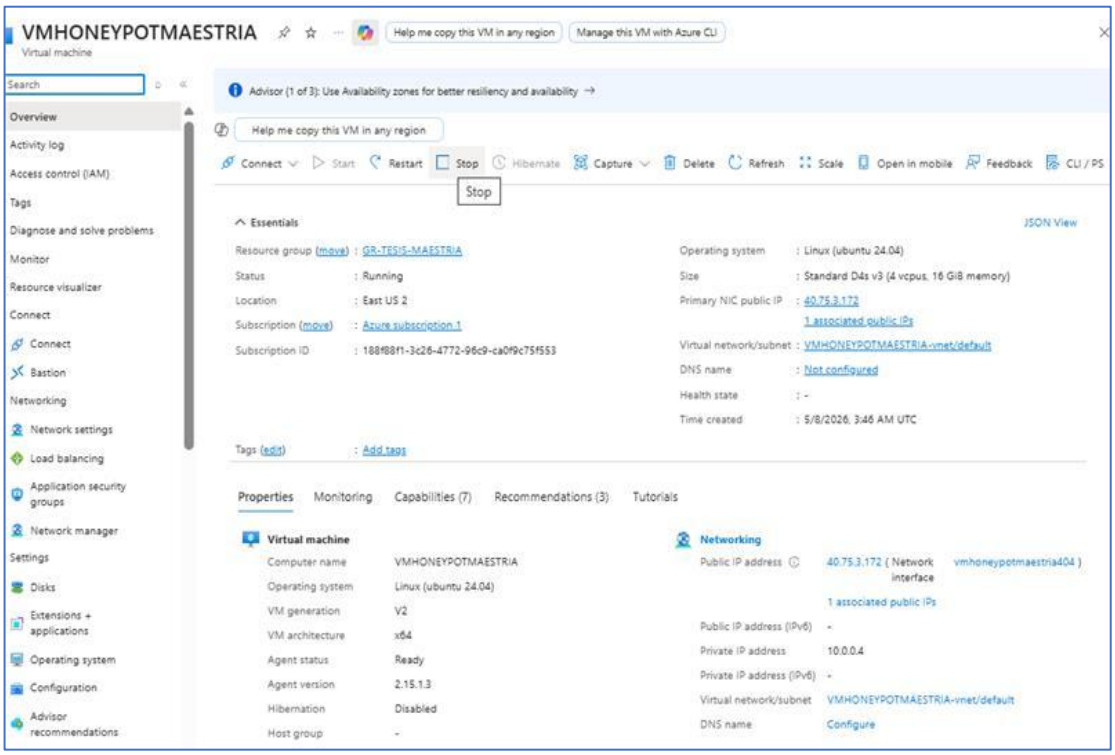
La máquina utilizará una plantilla D4s v3 con 4 vcpus, 16 Gb de Memoria y un disco SSD de 30 Gb, inicialmente se utilizó la plantilla D2s_v3 con 2 vcpus y 8gb de RAM pero la máquina se inhibía constantemente, tal como se indica en la Ilustración 16. revisando las métricas de recursos se notó que era necesaria una plantilla con mayores prestaciones.

Figura 18.

Consumo de CPU

Figura 19.

Validación VM Honeypot Maestría



3.2. Despliegue de Honeypot en Máquina Virtual

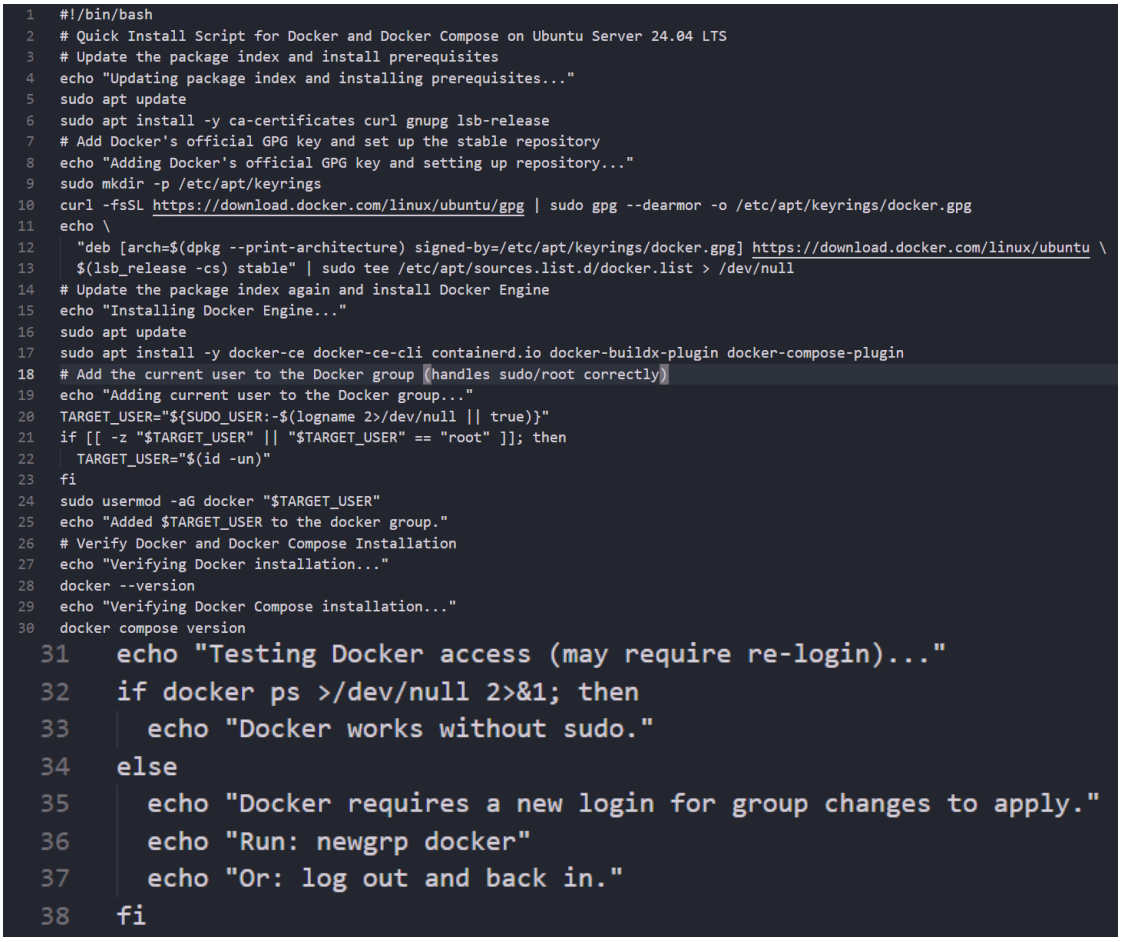
Una vez desplegada la Máquina se procederá a instalar el Honeypot de Cowrie, para esto se replicará de un repositorio de Github, para esto utilizamos el repositorio de T-POT, en primer lugar, se instalará el contenedor de Docker:

Figura 20.

Instalación de Docker

Figura 21.

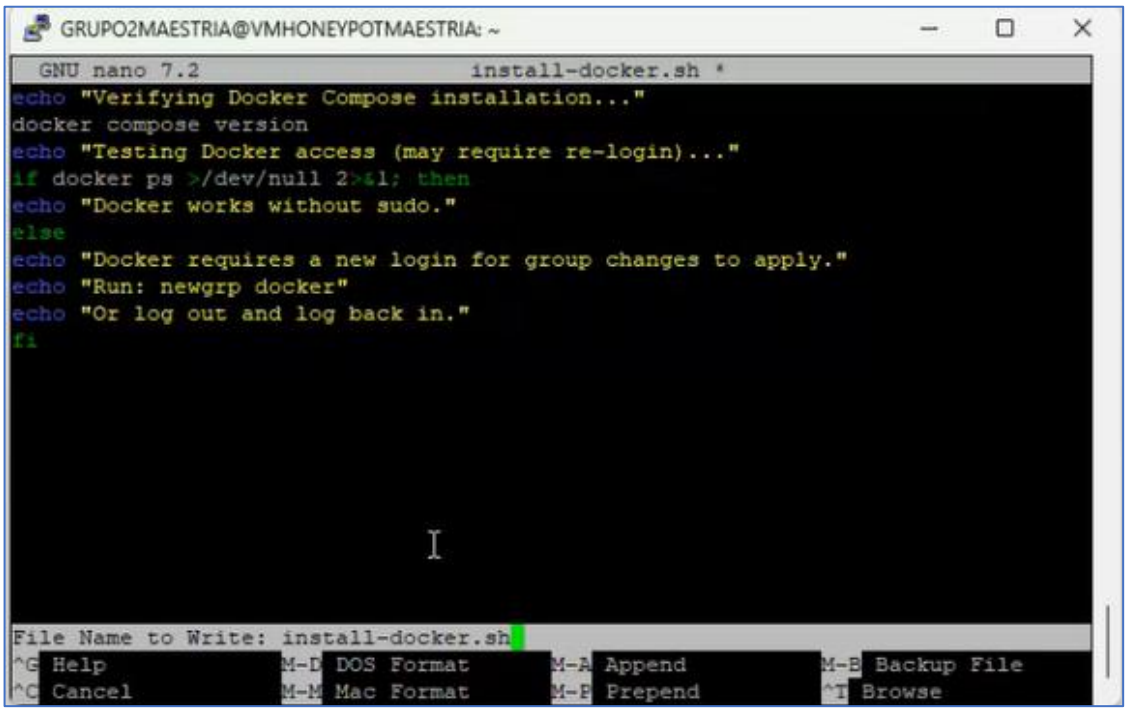
Código GitHub de instalación de Dockers



```
#!/bin/bash
# Quick Install Script for Docker and Docker Compose on Ubuntu Server 24.04 LTS
# Update the package index and install prerequisites
echo "Updating package index and installing prerequisites..."
sudo apt update
sudo apt install -y ca-certificates curl gnupg lsb-release
# Add Docker's official GPG key and set up the stable repository
echo "Adding Docker's official GPG key and setting up repository..."
sudo mkdir -p /etc/apt/keyrings
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /etc/apt/keyrings/docker.gpg
echo \
  "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.gpg] https://download.docker.com/linux/ubuntu \
  $(lsb_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null
# Update the package index again and install Docker Engine
echo "Installing Docker Engine..."
sudo apt update
sudo apt install -y docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin
# Add the current user to the Docker group (handles sudo/root correctly)
echo "Adding current user to the Docker group..."
TARGET_USER="${SUDO_USER:-$(logname 2>/dev/null || true)}"
if [[ -z "$TARGET_USER" || "$TARGET_USER" == "root" ]]; then
  TARGET_USER="$(id -un)"
fi
sudo usermod -aG docker "$TARGET_USER"
echo "Added $TARGET_USER to the docker group."
# Verify Docker and Docker Compose Installation
echo "Verifying Docker installation..."
docker --version
echo "Verifying Docker Compose installation..."
docker compose version
echo "Testing Docker access (may require re-login)..."
if docker ps >/dev/null 2>&1; then
  echo "Docker works without sudo."
else
  echo "Docker requires a new login for group changes to apply."
  echo "Run: newgrp docker"
  echo "Or: log out and back in."
fi
```

Figura 22.

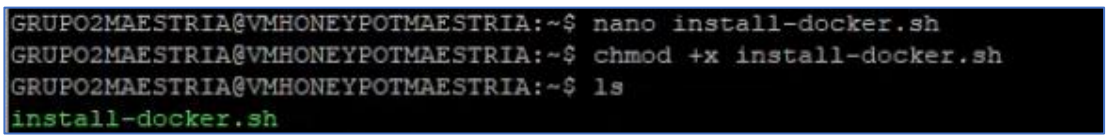
Verificación de Docker Compose



Luego se otorgó los permisos al instalador de Dockers con el comando chmod.

Figura 23.

Otorgación de permisos a Dockers

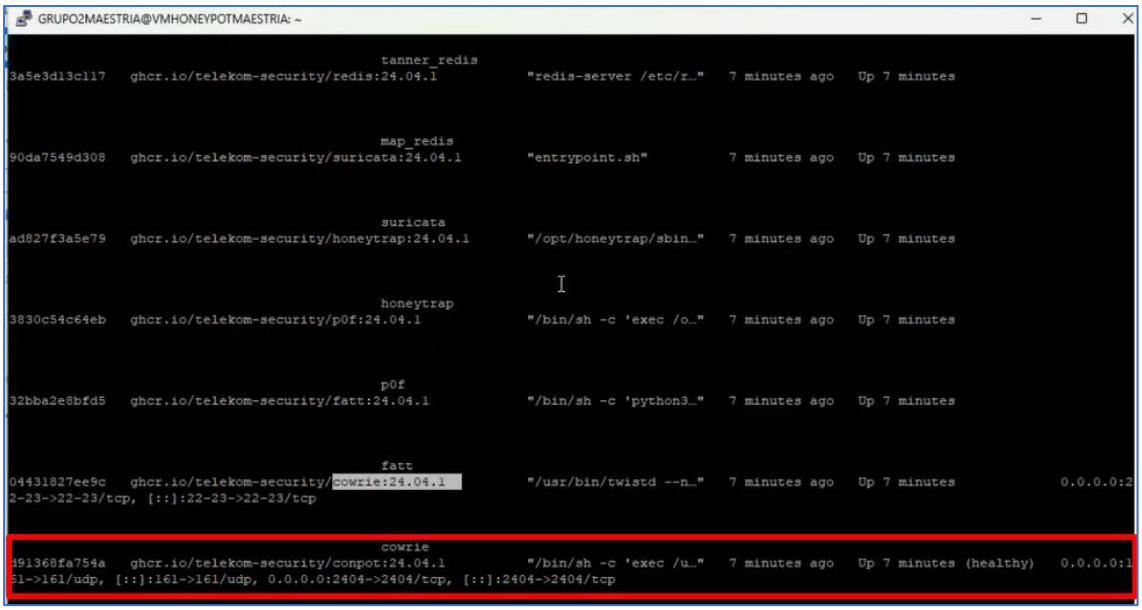


En la consola se visualiza el listado de contenedores activos dentro del entorno desplegado. Se observa que todos los contenedores se encuentran en estado operativo (“Up”), lo que indica que los servicios están funcionando correctamente. El contenedor Cowrie presenta un estado “healthy”, lo cual confirma su correcto funcionamiento y su disponibilidad para la captura de eventos asociados a posibles actividades maliciosas.

Posteriormente, se procedió a desactivar los demás contenedores, manteniendo únicamente el servicio de Cowrie activo. Esta acción tuvo como objetivo aislar el honeypot principal dentro del entorno, optimizando el consumo de recursos y permitiendo enfocar el análisis exclusivamente en los eventos generados por este sensor específico.

Figura 24.

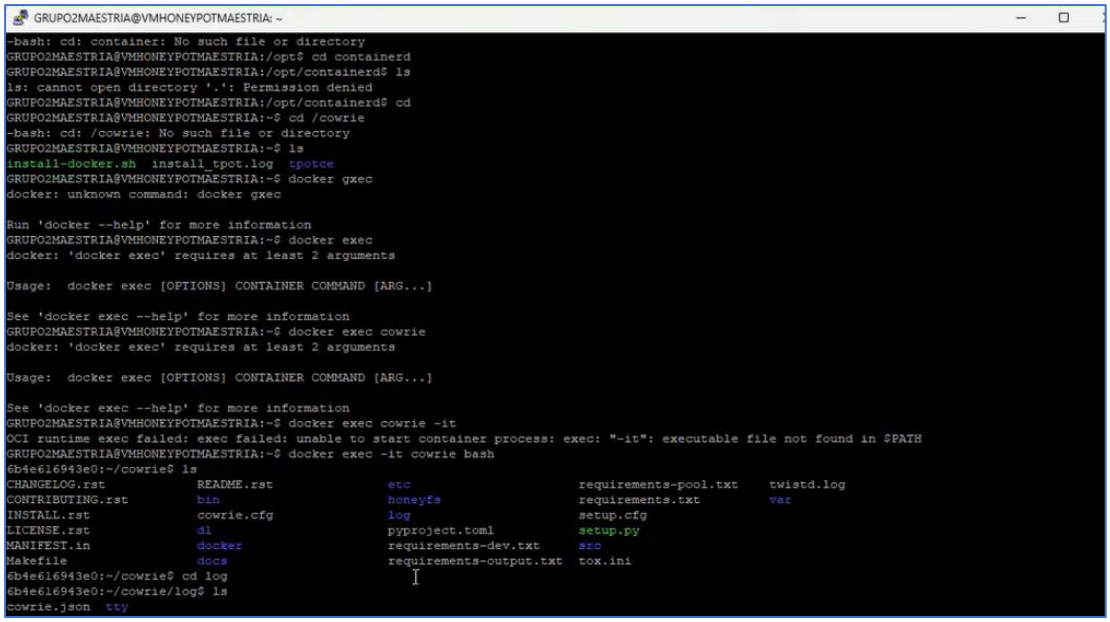
Estado de contenedores del honeypot en Docker con Cowrie activo y operativo.



Se logra acceder al contenedor correspondiente a Cowrie y navegar dentro de su estructura de archivos, donde se identifican directorios y archivos relevantes como log, cowrie.cfg, requirements.txt y twistd.log. Esta interacción permite validar el correcto despliegue del honeypot y la disponibilidad de los logs generados, los cuales son fundamentales para su posterior ingesta y análisis en Microsoft Sentinel. En conjunto, la captura evidencia el proceso de verificación y acceso al entorno operativo del honeypot, elemento clave dentro de la arquitectura de monitoreo implementada.

Figura 25.

Interacción con el contenedor Cowrie a través de Docker para la verificación de directorios, configuración y logs del honeypot.

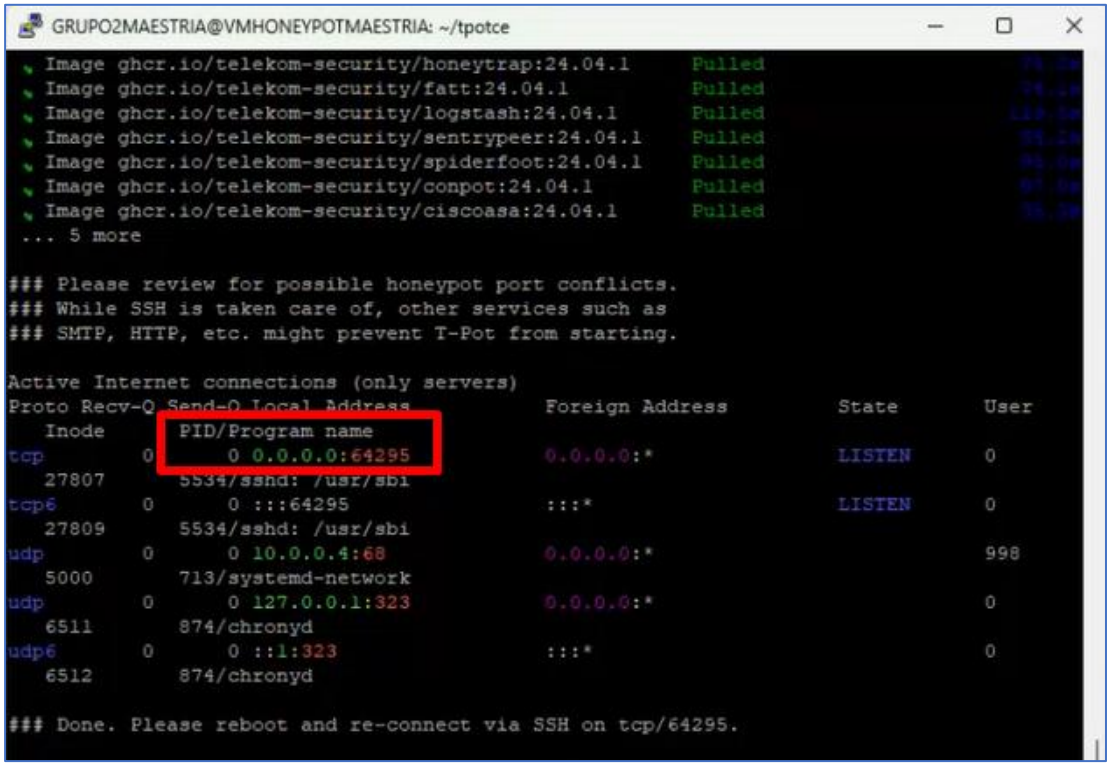


En la consola se evidencia que el servicio SSH se encuentra escuchando en el puerto 64295, en lugar del puerto estándar 22. Esta modificación corresponde a la configuración aplicada por el entorno. con el objetivo de evitar conflictos entre servicios y permitir la correcta operación de los honeypots desplegados.

Asimismo, se observa el mensaje generado por el sistema indicando la necesidad de reiniciar la conexión mediante SSH utilizando el nuevo puerto configurado (“Please reboot and re-connect via SSH on tcp/64295”). Esto confirma que el acceso administrativo a la máquina virtual deberá realizarse a través de este puerto no estándar, garantizando la continuidad de la gestión del entorno.

Figura 26.

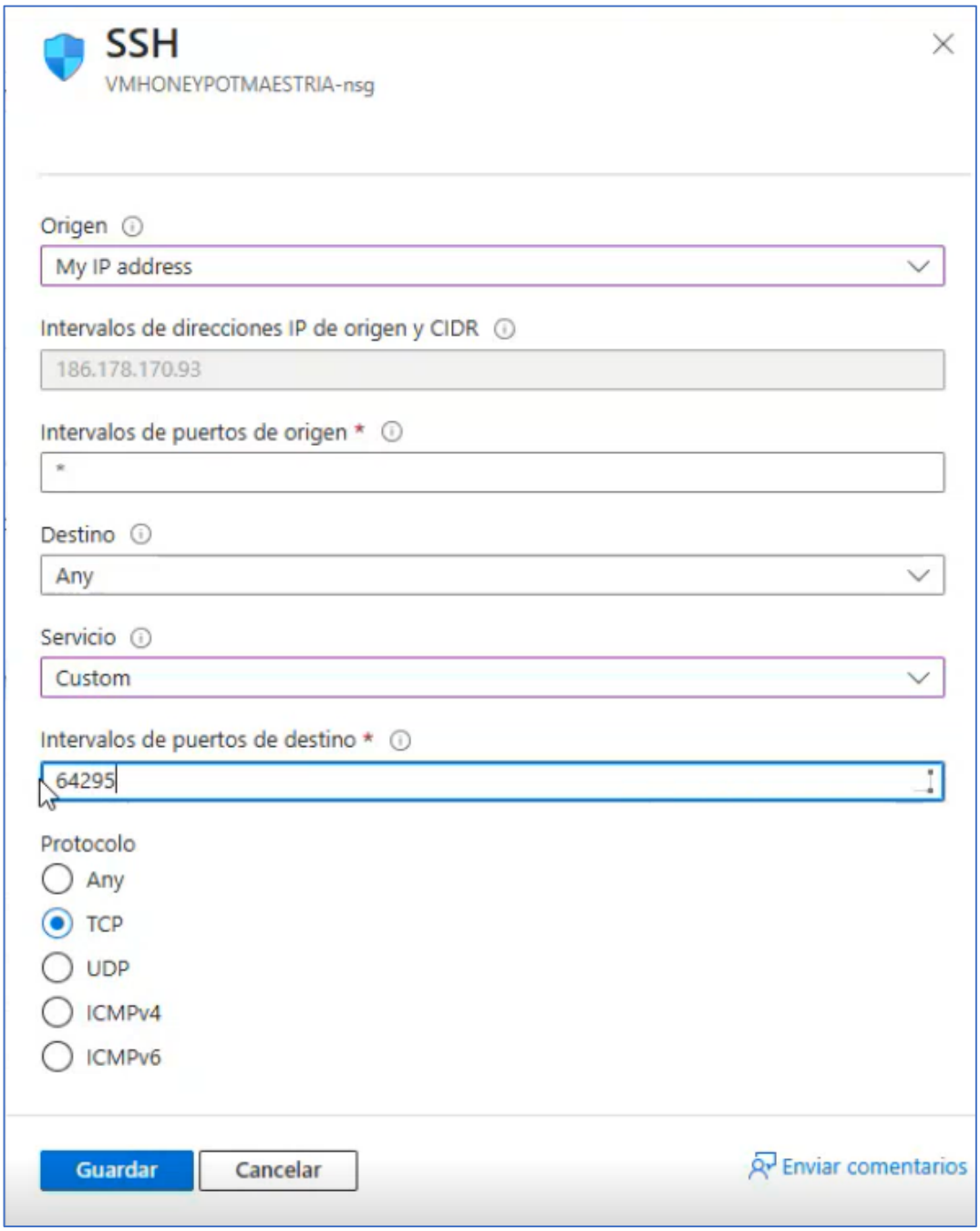
Configuración del puerto SSH en 64295 y ajuste de reglas NSG para permitir la conectividad.



La imagen evidencia que el servicio SSH fue configurado en el puerto 64295, en lugar del puerto estándar 22. Debi*do a este cambio, se realizó la modificación de las reglas del Network Security Group (NSG) para permitir el acceso remoto mediante dicho puerto y garantizar la conectividad con la máquina virtual.*

Figura 27.

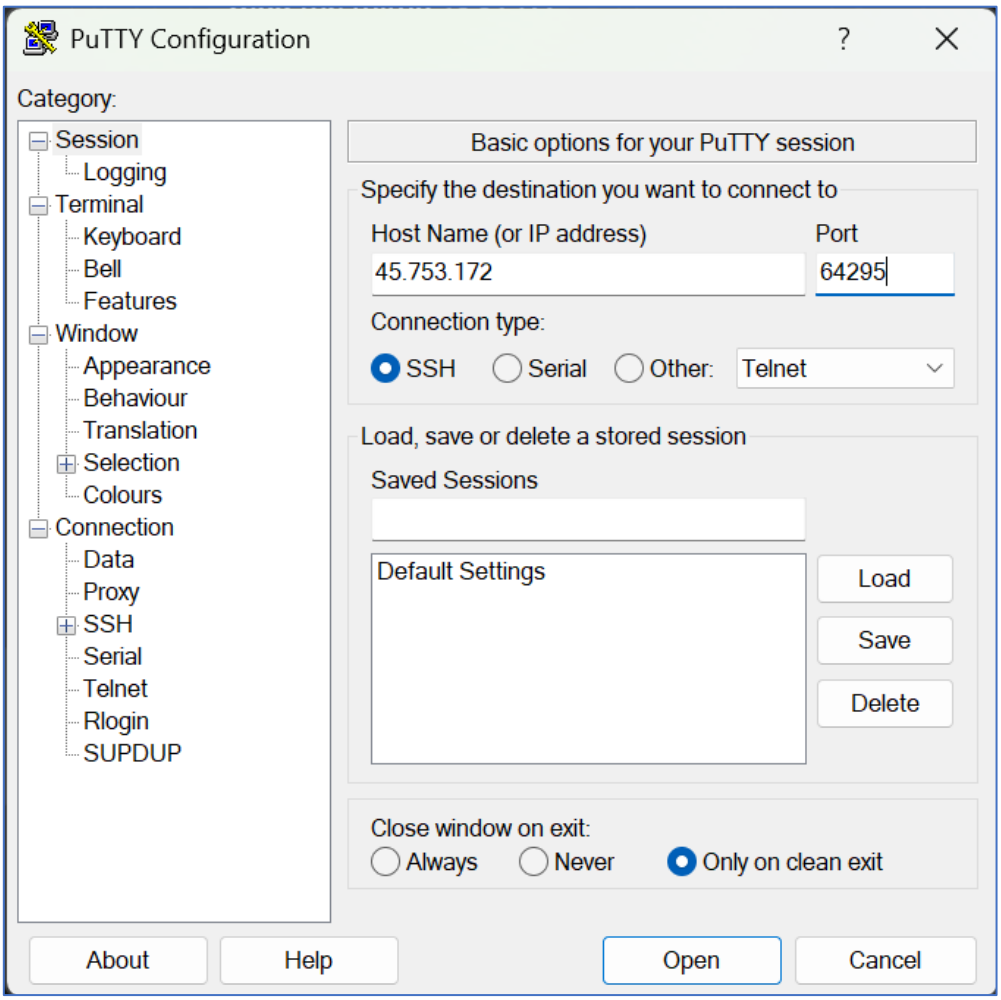
Habilitación del SSH en regla NSG



Luego, se probó la conexión mediante Putty en el puerto 64295 con la ip publica de la máquina virtual, tal como se configuró en la siguiente ilustración:

Figura 28.

Pruebas de acceso SSH



De la misma forma al ser un Honeypot que capta intentos de conexión SSH y Telnet es necesario abrir los puertos 22 y 23 a cualquier Ip y restringir únicamente el puerto nuevo (64295) para conexión SSH, esto lo podemos lograr con dos reglas NSG ejecutadas por prioridad, la primera regla permitirá únicamente el acceso por el puerto 64295 a la ip desde donde queremos conectarnos durante ese momento, es decir simulamos un acceso Just In Time, por otro lado la segunda regla permite acceso al puerto 22 simulando una maquina vulnerable a cualquier ip (Any) , finalmente en el puerto 64295 podemos validar que se encuentra corriendo el contenedor para el Honeypot de Cowrie:

Figura 29.

Validación de Contenedor de Cowrie

A manera de resumen y para evitar confusiones, tenemos la siguiente tabla con los puertos utilizados y su función.

Tabla 1.

Uso de puertos en sistema cowrie

Puerto	Propósito	Origen permitido	Destino	Riesgo controlado
22	Servicio SSH emulado por Cowrie	Any (Internet)	Honeypot Cowrie	El acceso se limita al servicio emulado; no existe acceso al sistema operativo anfitrión.
23	Servicio Telnet emulado por Cowrie	Any (Internet)	Honeypot Cowrie	Permite capturar actividad maliciosa sin comprometer el servidor real.
64295	Acceso administrativo SSH al servidor de Azure	Únicamente la IP autorizada del administrador	Máquina virtual	Evita que el acceso administrativo quede expuesto a Internet y reduce el riesgo de accesos no autorizados.

- **Envío de Logs desde Maquina Honeypot a Sentinel**

Para realizar el envío de logs desde la máquina virtual, es necesario la creación de una tabla Custom, un Data Collection Rule y una muestra JSON de los logs del Honeypot que se puede extraer ingresando a la máquina virtual a través del puerto 64295.

En base a los logs de muestra extraídos se crea la tabla con las columnas obtenidas en el archivo de muestra, de donde se tiene el eventid asociado para indicar el tipo de actividad registrada, la ip origen, el puerto origen, el ip y el puerto destino, una id de la sesión, el protocolo, un mensaje, el sensor y la fecha del evento, Para los logs de Muestra se utilizaron los siguientes:

Figura 30.

Logs desde Maquina Honeypot a Sentinel

[

{"eventid":"cowrie.session.connect","src_ip":"125.120.11.57","src_port":35957,"dst_ip":"192.168.112.2","dst_port":23,"session":"6b791adf6a49","protocol":"telnet","message":"New connection: 125.120.11.57:35957 (192.168.112.2:23) [session: 6b791adf6a49]","sensor":"9c35914842bf","timestamp":"2026-05-13T14:47:35.260904Z"},

{"eventid":"cowrie.session.closed","duration":13.35191535949707,"message":"Connection lost after 13 seconds","sensor":"9c35914842bf","timestamp":"2026-05-13T14:47:48.612719Z","src_ip":"125.120.11.57","session":"6b791adf6a49"},

{"eventid":"cowrie.session.connect","src_ip":"174.95.208.251","src_port":42498,"dst_ip":"192.168.112.2","dst_port":23,"session":"851493ab3e47","protocol":"telnet","message":"New connection: 174.95.208.251:42498 (192.168.112.2:23) [session: 851493ab3e47]","sensor":"9c35914842bf","timestamp":"2026-05-13T14:54:16.583869Z"},

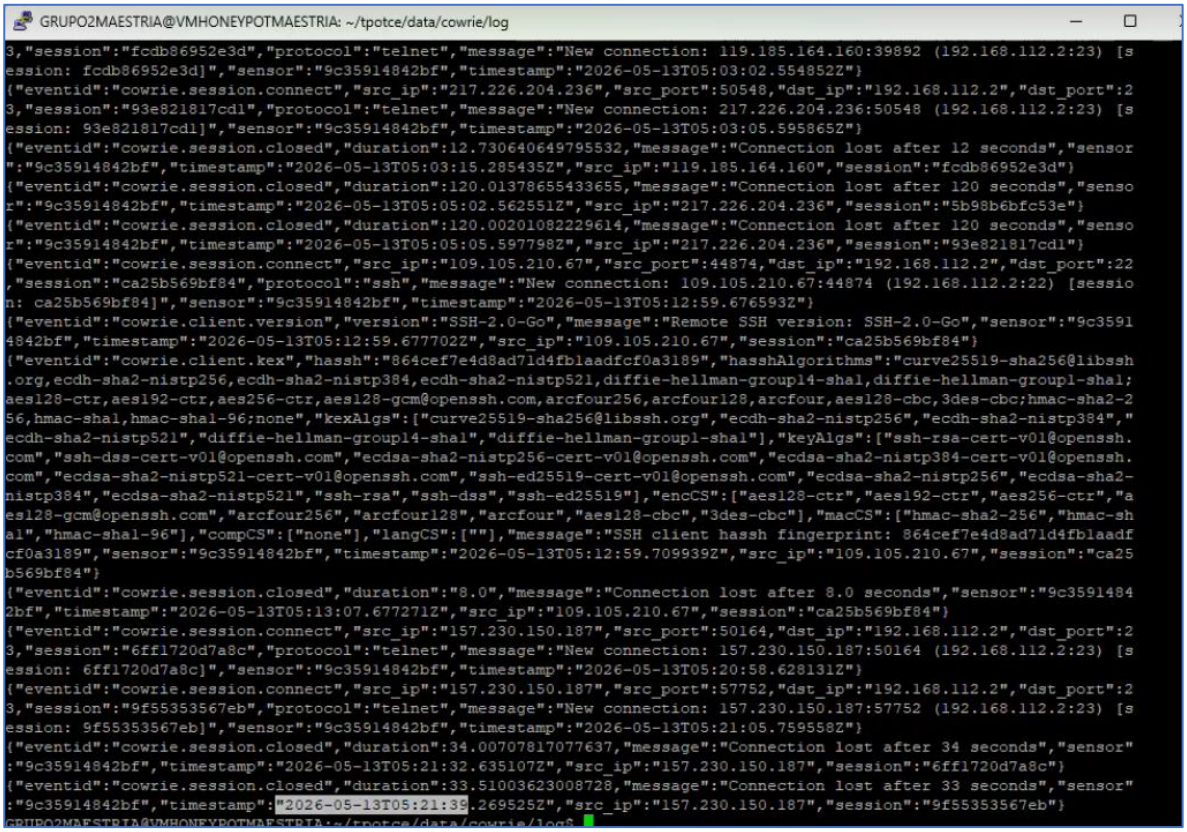
{"eventid":"cowrie.session.closed","duration":13.374595642089844,"message":"Connection lost after 13 seconds","sensor":"9c35914842bf","timestamp":"2026-05-13T14:54:29.958382Z","src_ip":"174.95.208.251","session":"851493ab3e47"}

]

Para obtener la ruta, se navegó dentro de la maquina hasta encontrar la ruta donde se almacenan los logs del cowrie para nuestro caso /tpot/data/cowrie/log.

Figura 31.

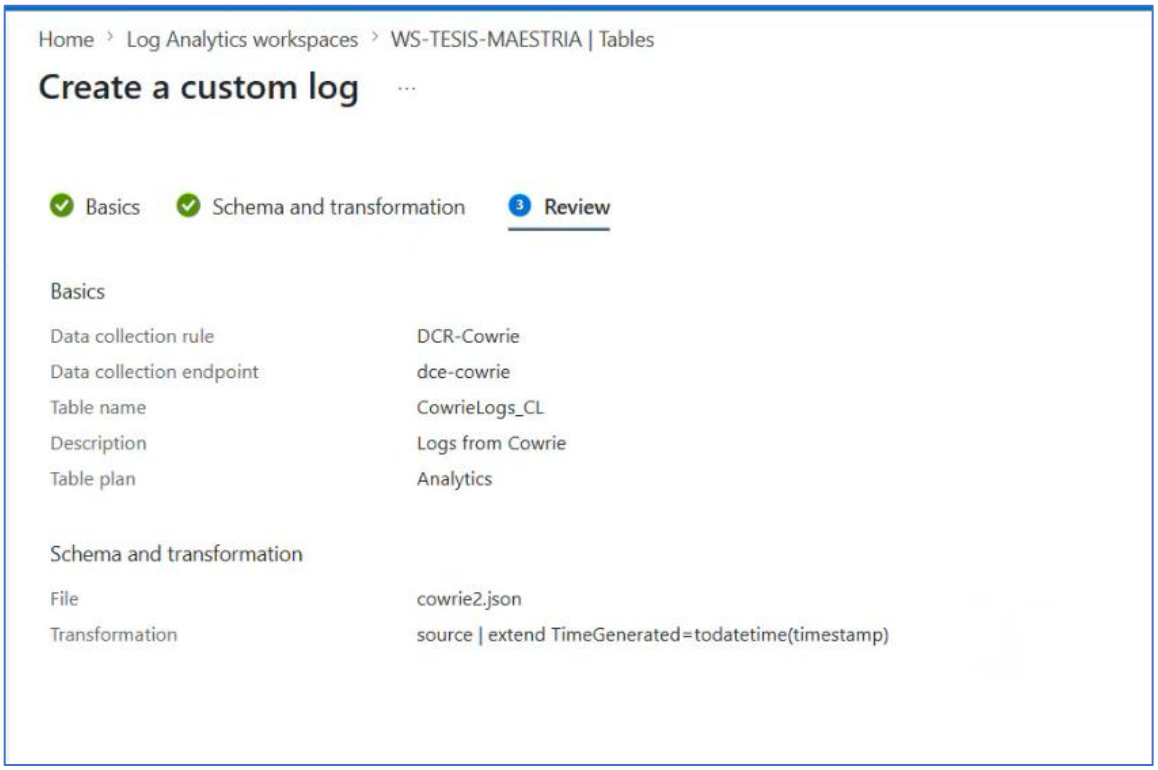
Logs de Cowrie en Máquina Virtual



Mientras que para la creación de la tabla se configuro el nombre de la tabla Custom (CowrieLogs_CL), la muestra de logs (cowrie2.json) y la transformación para generar una columna “TimeGenerated” necesaria para crear la tabla.

Figura 32.

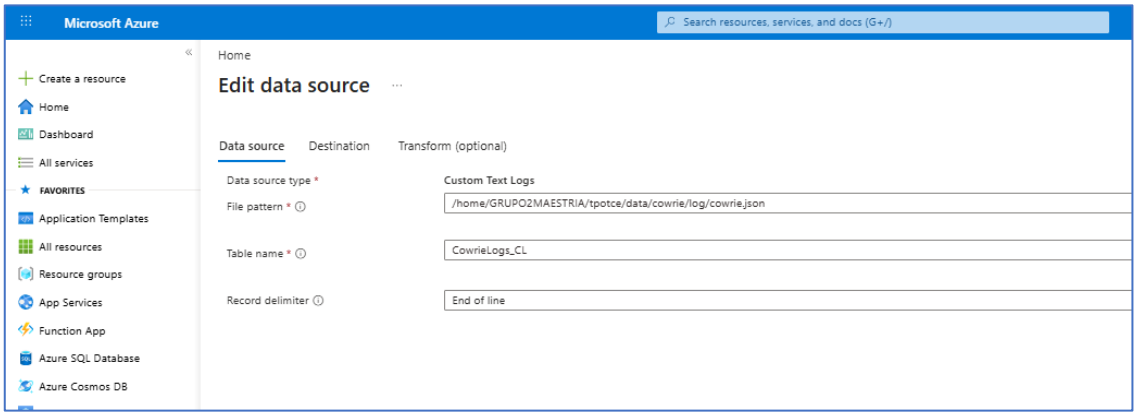
Creación de Tabla Custom



Mientras que para la configuración del Data Collection Rule se utilizó la siguiente configuración:

Figura 33.

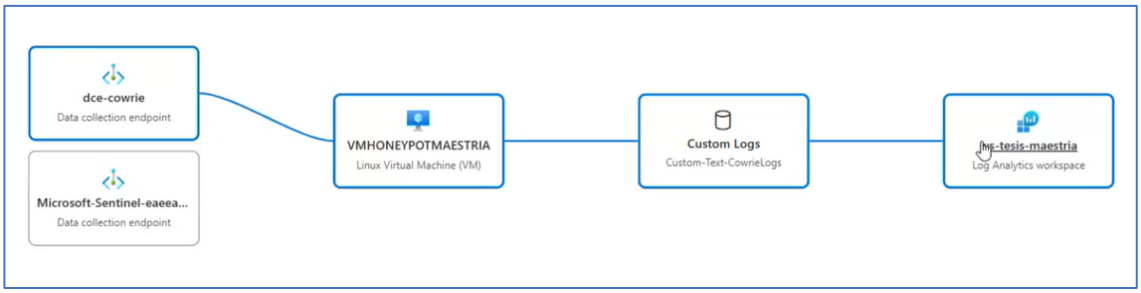
Configuración de Data Collection Rule



Con esta configuración se indicó que los logs se encuentran en la ruta que se encontró previamente, en que tabla se enviarán y cuál será el delimitador de cada log, para nuestro caso el fin de una línea. El resumen de envió de logs desde la maquina a Sentinel se puede resumir en el siguiente diagrama:

Figura 34.

Diagrama de conexión



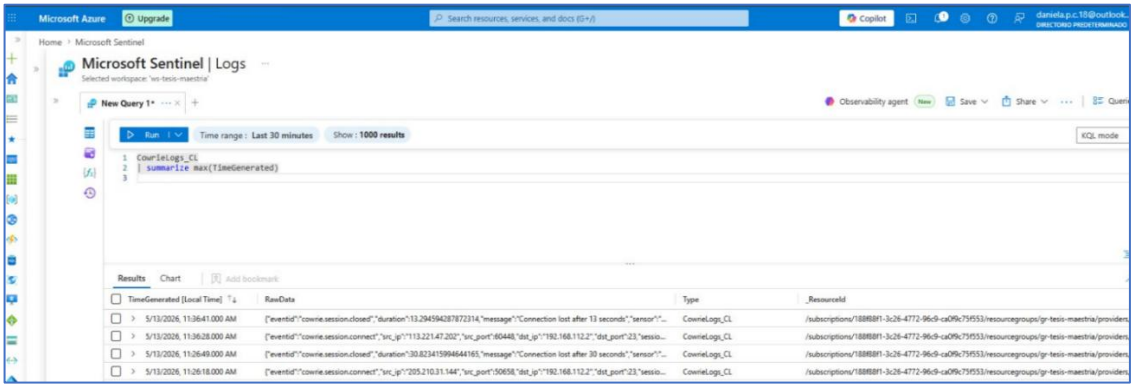
En esta arquitectura se indica que los logs que llegan de la máquina virtual pasan por el Data Collection Endpoint hacia la tabla Custom que se ingestará en el Sentinel del Log Analytics Workspace (ws-tesis-maestria).

- **Verificación de Recepción de Logs de Honeypot**

Una vez configurado el Data Collection Rule e ingestando los logs del Honeypot de Cowrie, se pueden visualizar en la sección de “Logs” de Microsoft Sentinel con la ejecución de una query KQL.

Figura 35.

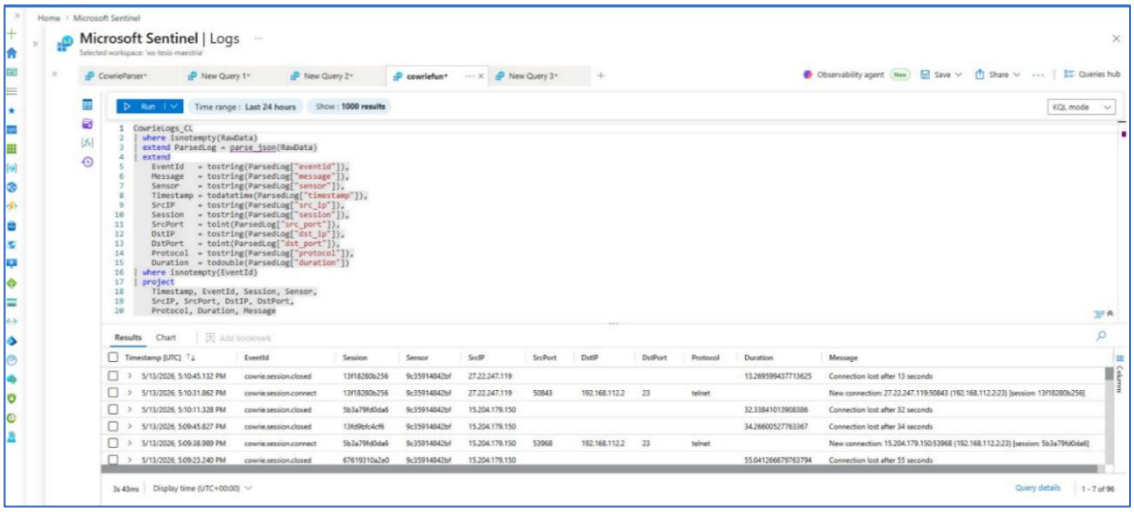
Validación de Logs de Cowrie



Dado que los logs llegan en formato Syslog en una única columna (RawData), se creó una función para poder pasar los datos en columnas separadas para poder visualizar la información de mejor manera y posteriormente crear consultas KQL que puedan realizar distintas correlaciones:

Figura 36.

Parseo de Logs de Honeypot Cowrie



Esta función separa por las columnas de EventId (Tipo de evento), Session (Id de Sesión), Sensor (Tipo de sensor que realizo la detección), SrcIP(Ip Origen), SrcPort(Puerto

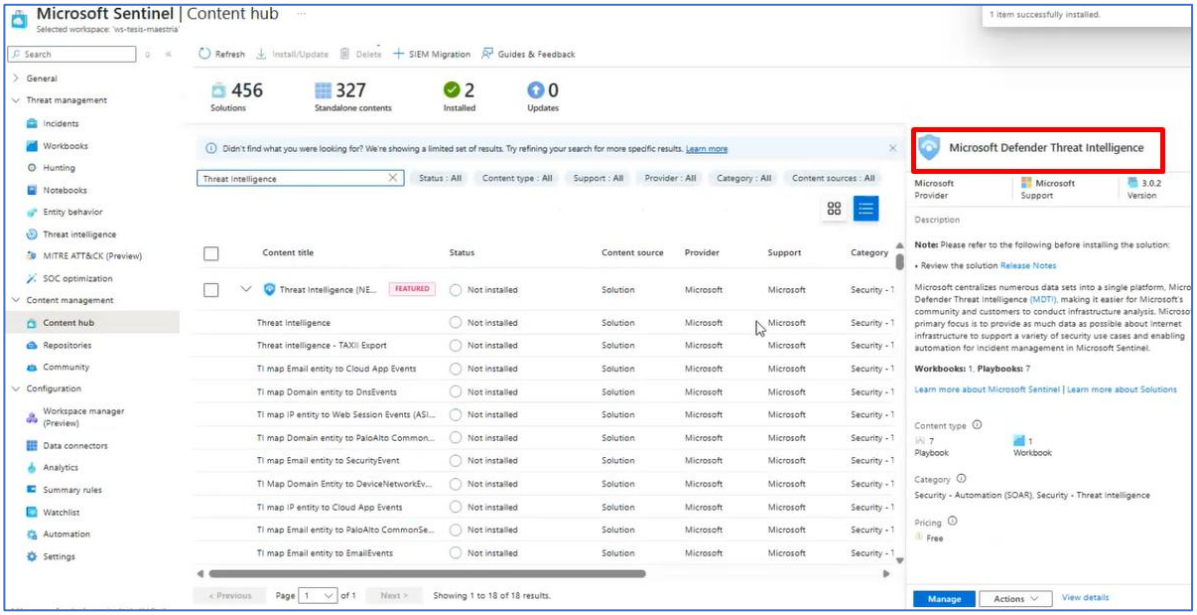
Origen), DstIp (Ip Destino), DstPort(Puerto Destino), Protocol(Protocolo), Duration (Duración de la conexión) y Message (mensaje asociado donde se incluirá el comando si está presente).

3.3 Despliegue de Conectores

Para la ingesta de Logs de Inteligencia de amenazas de Microsoft Defender Threat Intelligence, se procedió a instalar el conector de “Microsoft Defender Threat Intelligence”, esta tabla ingesta los logs generados por las fuentes de Inteligencia de Microsoft Defender, Incluye tags, confidencia, el indicador, el tlp y el tipo de fuente origen, toda esta información se ingesta en la tabla “ThreatIntelIndicators” que se detalla más granular en la Ilustración 34.

Figura 37.

Conector Microsoft Defender Threat Intelligence en Content Hub

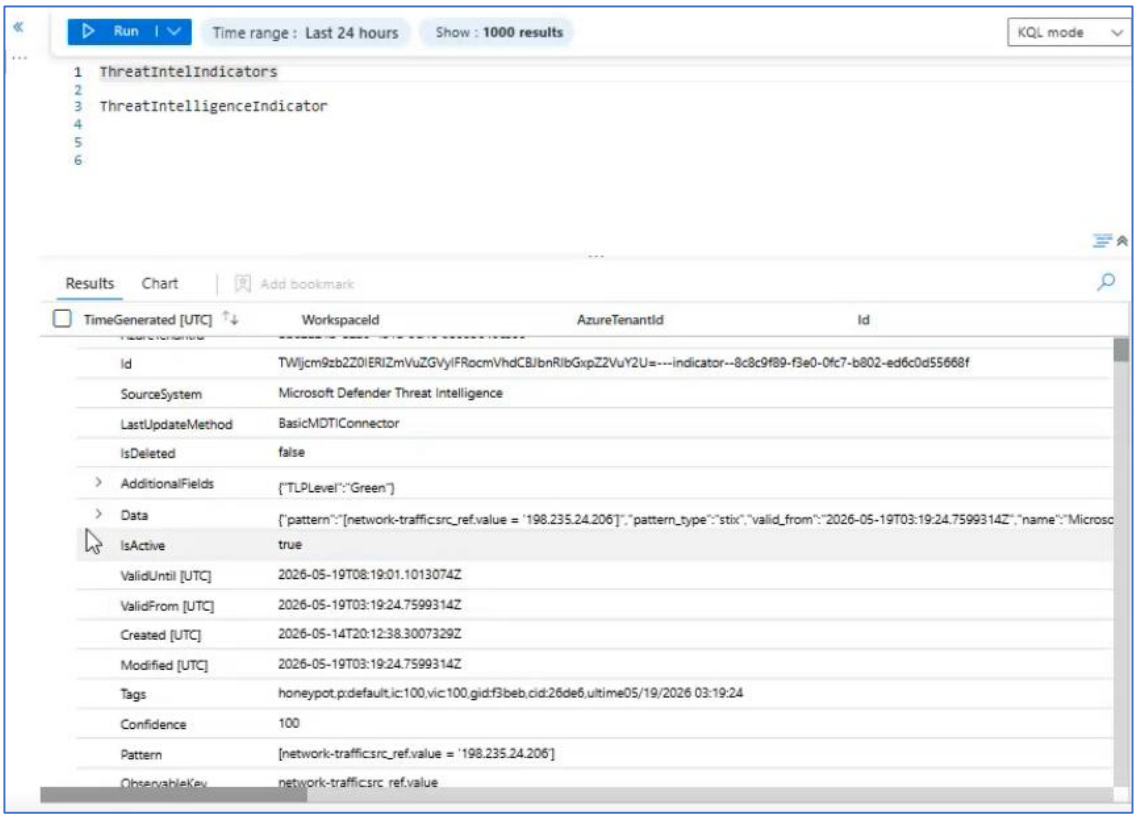


- **Verificación de Recepción de Logs de Threat Intelligence**

  Una vez activado el conector se puede obtener los logs similares al siguiente:

Figura 38.

Validación de campos en tabla Threat Intel Indicator



En este caso nos indica información relacionada con la hora de la ingesta del log, un id, la fuente, como se actualizo, el TLP utilizado para divulgar el IOC, la información en formato JSON tomada de formato STIX utilizado, la fecha de validación del Indicador y los tags que indican que fuente realizo la detección en nuestro ejemplo un honeypot de Microsoft, además del valor de la confiabilidad del Indicador según las fuentes de la herramienta.

- **Creación de Consulta KQL para Comparación de Logs en tabla Threat Intelligence y Cowrie**

Se creo sentencias KQL para poder validar la cantidad de Indicadores que aparecen en la tabla ThreatIntelIndicators, en ambas tablas y únicamente los IOCs ingestados por la tabla CowrieLogs_CL:

Figura 39.

Consulta KQL para validación procedencia indicadores de compromiso.

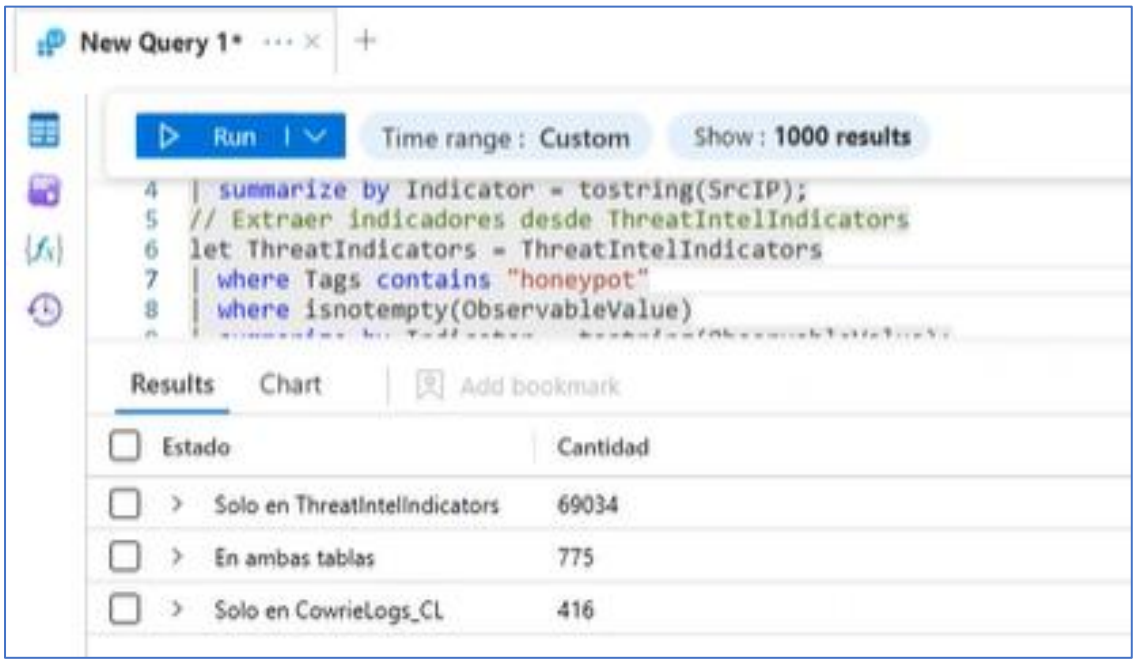
```
let CowrieLogs =
CowrieLogs_CL
| extend SrcIp = tostring(parse_json(RawData).src_ip)
| where isnotempty(SrcIp)
| summarize by Indicator = SrcIp;
// Extraer indicadores desde Threat Intelligence
let ThreatIndicators =
ThreatIntelIndicators
| where isnotempty(ObservableValue)
| summarize by Indicator = tostring(ObservableValue);
// Comparar ambas tablas
ThreatIndicators
| join kind=fullouter CowrieLogs on Indicator
| extend Estado = case(
    isnotempty(Indicator) and isnotempty(Indicator1), "En ambas tablas",
    isnotempty(Indicator) and isempty(Indicator1), "Solo en ThreatIntelIndicators",
    isempty(Indicator) and isnotempty(Indicator1), "Solo en CowrieLogs_CL",
    "Otro"
)
| summarize Cantidad = count() by Estado

```

De donde se obtuvo los siguientes resultados:

Figura 40.

Query KQL para conteo de eventos por tabla



- **Conteo de Logs en Tabla Threat Intelligence de Microsoft**

Para realizar el conteo de los eventos diarios ingestados por la tabla de Threat Intelligence de Microsoft, se creó la consulta KQL incluyendo la tabla, se realizó un filtro de los eventos con el tag de “Honeypot” y se realizó un summarize para contar por día los eventos, de donde se obtuvo entre 15 y 43 mil eventos diarios.

Tabla 2.

Tabla Threat Intelligence de Microsoft

TimeGenerated	count_
2026-06-04T00:00:00Z	604
2026-06-03T00:00:00Z	4062
2026-06-02T00:00:00Z	3342
2026-06-01T00:00:00Z	3771
2026-05-31T00:00:00Z	114497
2026-05-30T00:00:00Z	5342
2026-05-29T00:00:00Z	14892
2026-05-28T00:00:00Z	13345
2026-05-27T00:00:00Z	26499
2026-05-26T00:00:00Z	4729
2026-05-25T00:00:00Z	3513
2026-05-24T00:00:00Z	126292
2026-05-23T00:00:00Z	5956
2026-05-22T00:00:00Z	14321
2026-05-21T00:00:00Z	15611
2026-05-20T00:00:00Z	25239
2026-05-19T00:00:00Z	39110

2026-05-18T00:00:00Z	42419
2026-05-17T00:00:00Z	131039

Figura 41.

Rango de resultados tabla Threat Intelligence

- **Conteo de Logs en Tabla CowrieLogs**

Mientras que el Honeypot varía entre 15 mil y 28 mil eventos aproximadamente al día.

Tabla 3.

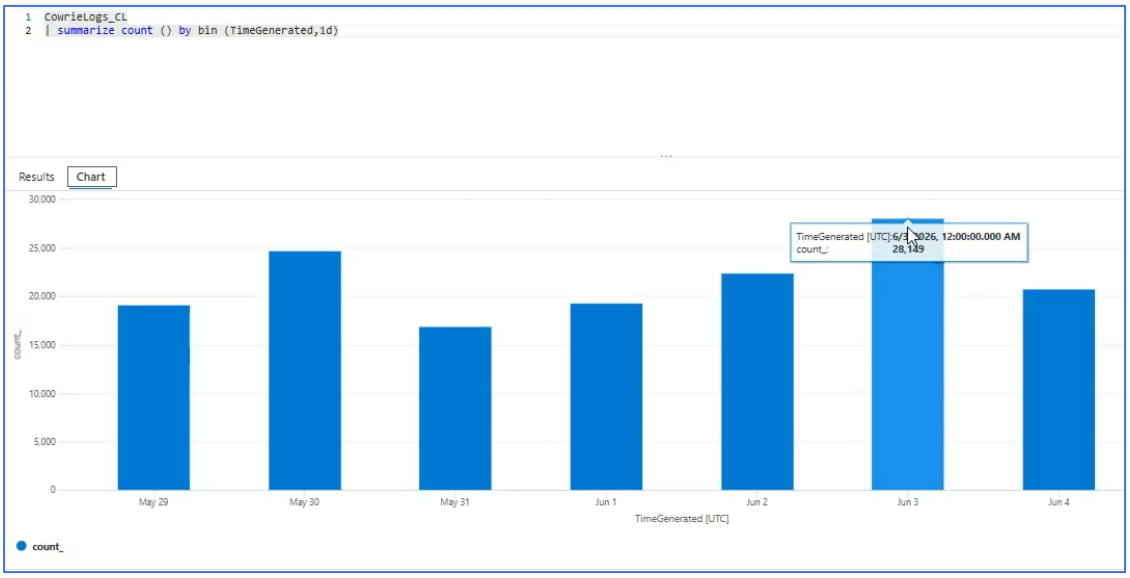
Tabla CowrieLogs

TimeGenerated	count_
2026-06-04T00:00:00Z	20762
2026-06-05T00:00:00Z	1441
2026-05-17T00:00:00Z	1046
2026-05-19T00:00:00Z	17120
2026-06-01T00:00:00Z	19354
2026-06-02T00:00:00Z	22478
2026-05-22T00:00:00Z	29
2026-06-03T00:00:00Z	28149
2026-05-30T00:00:00Z	24730
2026-05-31T00:00:00Z	16953
2026-05-24T00:00:00Z	365

2026-05-26T00:00:00Z	10031
2026-05-28T00:00:00Z	27327
2026-05-29T00:00:00Z	22490
2026-05-20T00:00:00Z	3510
2026-05-21T00:00:00Z	3
2026-05-27T00:00:00Z	15653

Figura 42.

Eventos por día tabla Honeypot Cowrie



- **Construcción de Consulta KQL para conteo de resultados y comparación de tablas**

Se construyó una consulta, la cual valida en la tabla de Cowrie diversos comandos que utiliza un atacante para realizar un escaneo en la fase de reconocimiento, entre los cuales se tiene (wget, curl, chmod, nc, ncat, bash, sh, Python, perl, nmap, ssh, scp) esta consulta nos indicara la ip maliciosa, el número de comandos maliciosos y un valor booleano que indicara si esta Ip se encuentra en la tabla ThreatIntelIndicator o no (En el caso que el valor sea “NO” se asegura que la ip se detectó por el Honeypot y no esta ingestada en las fuentes de Microsoft Sentinel), esto nos indica que un indicador fue detectado por la maquina honeypot y no por las

fuentes de Inteligencia de Defender. Como se puede validar en la siguiente Ilustración los comandos ejecutados buscan encontrar las contraseñas de la maquina:

Figura 43.

Código KQL para comparación de tablas de Inteligencia de Amenazas

```
let TimeFrame = 24h;
// Extraer comandos ejecutados
let CommandsExecuted =
cowriefun
| where Timestamp >= ago(TimeFrame)
| where Message startswith "CMD:"
| extend Command = trim(@" ", replace_string(Message, "CMD:", ""))
| summarize
    Commands = make_set(Command, 100),
    TotalCommands = count()
    by SrcIP;
// Detectar comandos sospechosos
let SuspiciousCommands =
cowriefun
| where Timestamp >= ago(TimeFrame)
| where Message startswith "CMD:"
| extend Command = trim(@" ", replace_string(Message, "CMD:", ""))
| where Command has_any (
    "wget",
    "curl",
    "chmod",
    "nc ",
    "ncat",
    "bash",
    "sh ",
    "python",
    "perl",
    "busybox",
    "tftp",
    "ftpget",
    "scp",
    "ssh",
    "nohup",
    "./"
)
| summarize
    SuspiciousList = make_set(Command, 100),
    SuspiciousCount = count()
    by SrcIP;
// Threat Intelligence
let ThreatIntel =
ThreatIntelIndicators
| where isnotempty(ObservableValue)
| extend ConfidenceScore = tostring(Data.confidence)
| extend Description = tostring(Data.description)
| summarize
    TI_Description = make_set(Description, 5),
    TI_Tags = make_set(Tags, 10),
    TI_Confidence = max(ConfidenceScore)
    by ObservableValue;
// Correlación final
CommandsExecuted
| join kind=leftouter SuspiciousCommands on SrcIP
| join kind=leftouter (
    ThreatIntel
    | project ObservableValue, TI_Description, TI_Tags, TI_Confidence
) on $left.SrcIP == $right.ObservableValue
| extend
    SuspiciousCount = coalesce(SuspiciousCount, 0)
```

```
| extend
    TI_Match = iff(isnotempty(ObservableValue), "YES", "NO")
| extend
    RiskLevel = case(
        TI_Match == "YES" and SuspiciousCount >= 5, "CRITICAL",
        TI_Match == "YES", "HIGH",
        SuspiciousCount >= 10, "HIGH",
        SuspiciousCount >= 5, "MEDIUM",
        TotalCommands >= 10, "LOW",
        "INFO"
    )
| project
    SrcIP,
    TotalCommands,
    SuspiciousCount,
    TI_Match,
    TI_Confidence,
    TI_Description,
    TI_Tags,
    Commands,
    SuspiciousList,
    RiskLevel
| order by
    case(
        RiskLevel == "CRITICAL", 5,
        RiskLevel == "HIGH", 4,
        RiskLevel == "MEDIUM", 3,
        RiskLevel == "LOW", 2,
        1
    ) desc,
    SuspiciousCount desc
```

Finalmente, se asigna en la Columna RiskLevel, un nivel de riesgo entre Low y Critical en base a si se encuentra en ambas tablas y el número de comandos sospechosos asociados a esa Ip, por lo tanto, se exponen las siguientes condiciones:

Tabla 4.

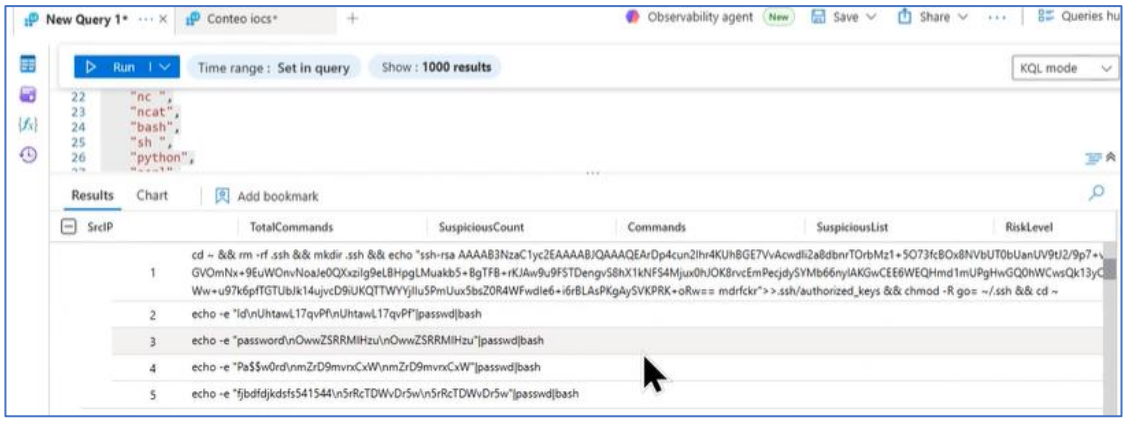
Consideraciones de Clasificación de Riesgo

Nivel de riesgo	Condición
CRITICAL	Coincidencia con Threat Intelligence **y** ≥ 5 comandos sospechosos
HIGH	Coincidencia con Threat Intelligence **o** ≥ 10 comandos sospechosos
MEDIUM	Entre 5 y 9 comandos sospechosos
LOW	≥ 10 comandos totales ejecutados
INFO	Ninguna de las condiciones anteriores

Entre los comandos que se encontró se puede notar diversos intentos de ejecución del comando echo en rutas donde se almacenan contraseñas.

Figura 44.

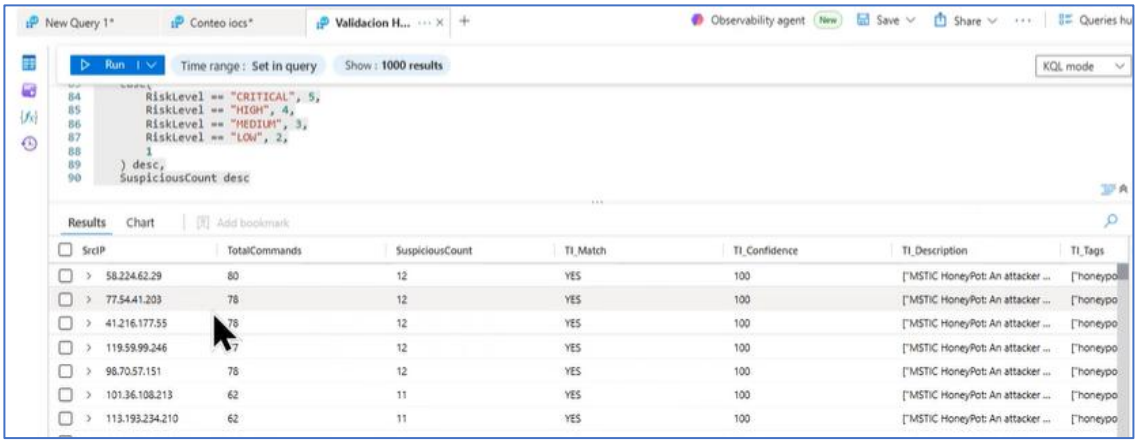
Validación de resultados query KQL



Mientras que el resultado de la consulta se muestra a continuación:

Figura 45.

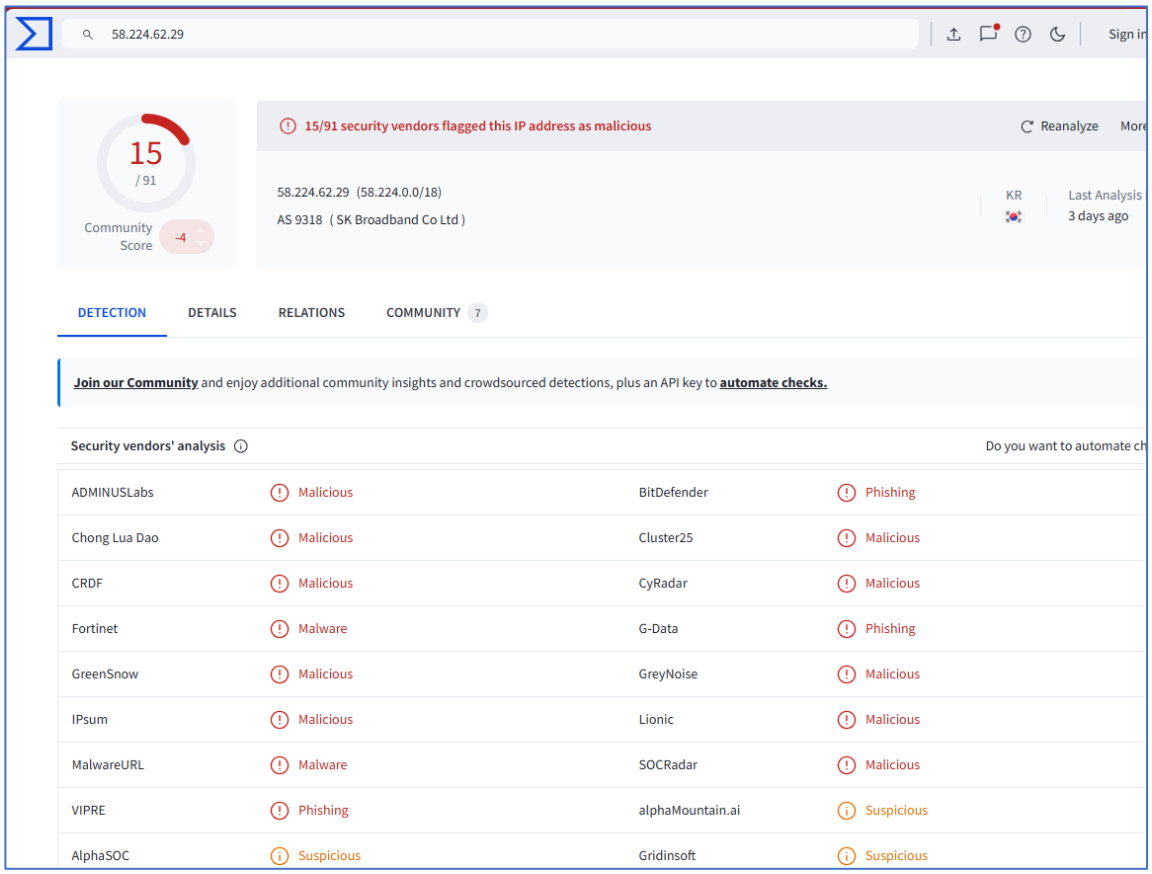
Detección de ips maliciosas



Para interpretar estos resultados se puede notar que se tiene la IP origen del escaneo, el número de comandos que se ejecutaron, el número de comandos catalogados como sospechosos, la columna “TI_Match” el cual es un booleano el cual indica si la IP se encuentra o no en las fuentes de Inteligencia del SIEM de Microsoft, el valor de Confidence y la descripción del log. Si tomamos la primera IP, podemos notar que efectivamente se cataloga como maliciosa:

Figura 46.

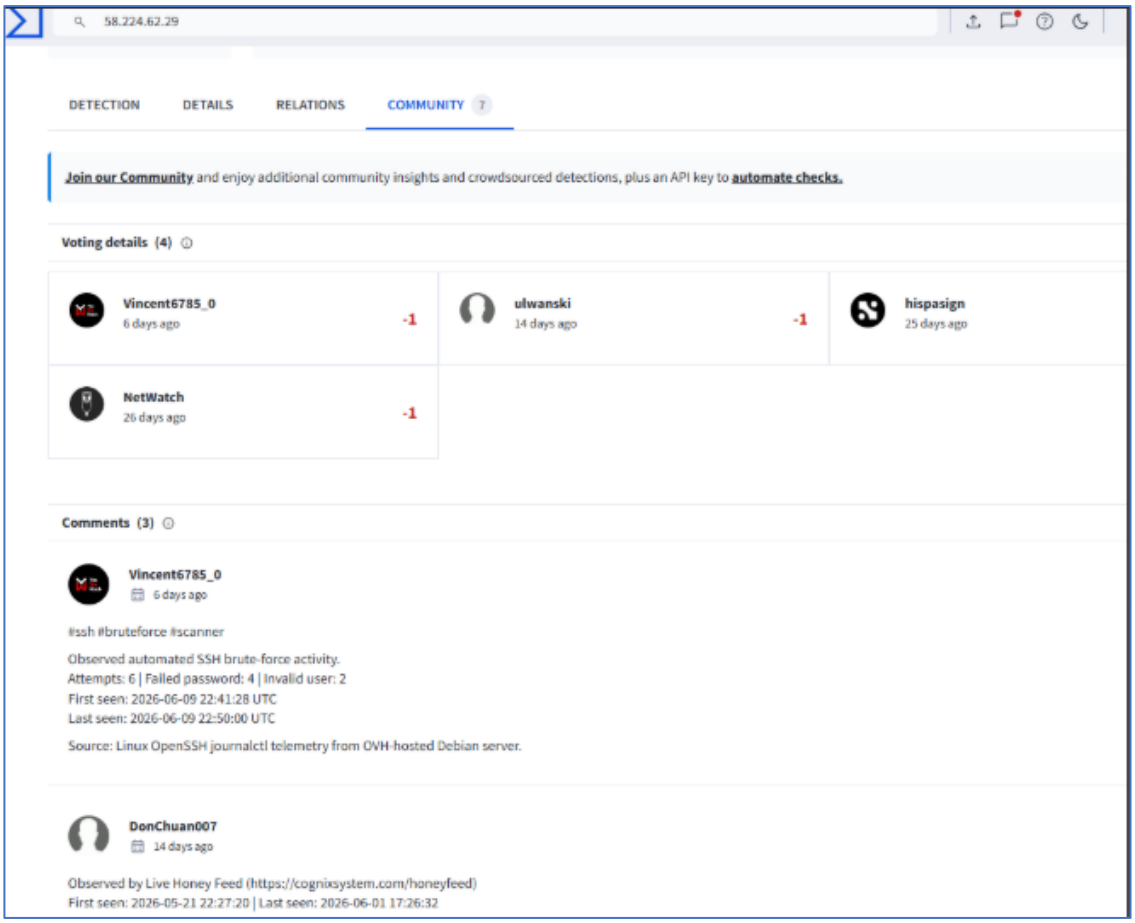
Revisión en virus total



Además de ser catalogada como maliciosa por 15 de 91 fuentes, se tiene varios comentarios de la comunidad las cuales catalogan la Ip en cuestión relacionada con escaneos ssh e intentos de ataques de fuerza bruta.

Figura 47.

Comentarios de Comunidad en Virus Total



3.4 Pruebas de Concepto

Como parte de las pruebas definidas en el alcance del proyecto, se realizó un escaneo de puertos utilizando la herramienta Nmap sobre la dirección IP pública del entorno desplegado. Los resultados mostraron los puertos 21, 22, 23, 42, 80 y 81 como accesibles o potencialmente vulnerables.

Figura 48.

Escaneo con nmap

De aquí podemos ver que el puerto para transferencia de archivos FTP y los puertos de navegación web http aparecen como puertos abiertos y escuchando, así como los puertos que permiten conexión remota como son el 22 y 23 para SSH y telnet respectivamente. Este comportamiento es el esperado. Por tanto, los servicios detectados no corresponden a vulnerabilidades reales de la infraestructura implementada, sino a mecanismos expuestos por el honeypot para simular un entorno atractivo para posibles atacantes.

Además, se realizó una prueba de acceso mediante el protocolo SSH utilizando las credenciales "root/root". La autenticación fue aceptada por el servicio emulado, permitiendo el acceso a un entorno controlado gestionado por Cowrie. Es importante destacar que dicho acceso no representa una intrusión real sobre un sistema productivo ni una vulnerabilidad efectiva de la infraestructura, sino una funcionalidad propia del honeypot, al realizar el ingreso a este entorno controlado se creó un archivo en el directorio home con un mensaje como lo muestra la ilustración 47.

Figura 49.

Prueba de Conexión SSH

Las pruebas de concepto descritas en esta sección tuvieron como finalidad verificar el correcto funcionamiento del entorno desplegado, comprobando que los servicios emulados por el honeypot fueran visibles desde Internet y que permitieran la interacción esperada con posibles atacantes dentro de un entorno completamente controlado. No obstante, los resultados principales analizados en esta investigación no se derivan únicamente de estas pruebas controladas, sino principalmente de la exposición del honeypot a Internet durante el período de observación definido en el proyecto. Durante dicho período, el sistema recibió múltiples intentos reales de reconocimiento, autenticación y ejecución de comandos provenientes de direcciones IP externas, cuyos eventos fueron capturados por Cowrie, enviados a Microsoft Sentinel y posteriormente analizados para identificar comportamientos maliciosos, tácticas y técnicas empleadas por los atacantes.

CAPÍTULO 4

4. ANÁLISIS DE RESULTADOS

4.1. Análisis de Resultados

4.1.1. Análisis de la ingesta de logs en Microsoft Sentinel

La presente sección analiza el comportamiento de la ingesta de logs generados en el entorno implementado, el cual integra un honeypot basado en Cowrie desplegado en Microsoft Azure y su posterior envío hacia Sentinel. La finalidad de este análisis es evaluar la contribución de las diferentes fuentes de datos dentro del sistema de monitoreo y su impacto en la detección de eventos de seguridad. La Ilustación 48. muestra la evolución de la ingesta de logs durante el periodo comprendido entre el 18 de mayo y el 3 de junio, representando el volumen de datos en gigabytes (GB) por día.

El eje horizontal representa la línea temporal en formato UTC, mientras que el eje vertical indica el volumen de datos ingeridos diariamente.

La información se presenta mediante un gráfico de barras que permite distinguir tres fuentes principales de registros:

- ThreatIntelligenceIndicators
- Syslog
- CowrieLogs_CL

A nivel general, se observa un comportamiento no uniforme en la ingesta de datos, evidenciando variaciones significativas entre los diferentes días analizados. En particular, se identifican picos de actividad relevantes alrededor del 18 y 24 de mayo, donde predomina ampliamente la contribución de ThreatIntelligenceIndicators, alcanzando valores cercanos a 0.34 GB y 0.36 GB respectivamente. Este comportamiento se asocia principalmente a la carga

de grandes volúmenes de indicadores de compromiso (IOCs) provenientes de fuentes externas integradas en Microsoft Sentinel.

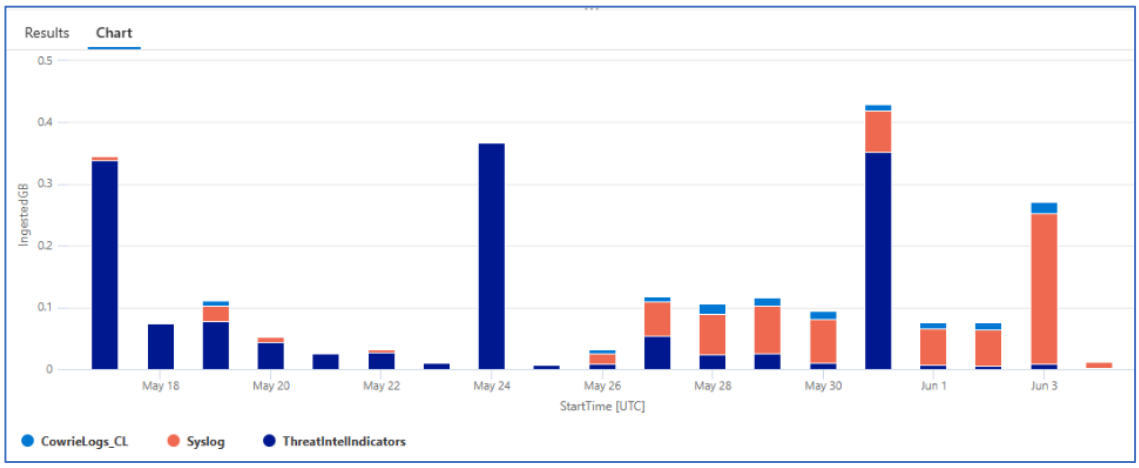
Asimismo, se identifica una tendencia creciente en la participación de los logs Syslog a partir del 28 de mayo, alcanzando su punto más representativo el 3 de junio, donde constituyen la mayor parte del volumen ingerido (aproximadamente 0.25 GB). Esta ingesta se relaciona a comportamiento y logs propios del equipo Ubuntu, tanto de sistema como de inicios de sesión.

En contraste, los registros provenientes del honeypot CowrieLogs_CL presentan una ingesta menor en comparación con las otras fuentes, manteniéndose constante a lo largo del periodo. Esta característica es coherente con la naturaleza de los honeypots de media interacción, los cuales generan eventos únicamente ante intentos reales de conexión o interacción maliciosa. Por lo tanto, su menor volumen no representa una limitación, sino una evidencia de que la información capturada está directamente relacionada con actividades potencialmente maliciosas, aportando un alto valor cualitativo al sistema de monitoreo.

En conjunto, el análisis de la imagen permite evidenciar la coexistencia de diversas fuentes de información, así como la variabilidad en su nivel de contribución a lo largo del tiempo. Esta interacción resulta fundamental para el proceso de correlación de eventos dentro de un sistema de monitoreo, ya que proporciona una visión integral del comportamiento del entorno. En este contexto, la combinación de múltiples tipos de logs facilita la identificación de patrones y tendencias, contribuyendo de manera significativa a la detección de posibles actividades maliciosas.

Figura 50.

Ingesta de logs en Microsoft Sentinel



La tabla presenta el volumen total de datos ingeridos en Microsoft Sentinel, expresado en gigabytes (GB), para tres fuentes principales: ThreatIntelligenceIndicators, Syslog y CowrieLogs_CL.

- **ThreatIntelligenceIndicators:** Concentra el mayor volumen de ingesta (≈1.54 GB), siendo la principal fuente de datos, debido a la carga masiva de indicadores de amenazas.
- **Syslog:** Con un volumen aproximado de (≈0.77 GB) aporta una cantidad significativa de información relacionada con la actividad operativa del sistema.
- **CowrieLogs_CL:** Presenta la menor ingesta (≈0.12 GB), lo cual es esperado, ya que el honeypot solo genera eventos ante interacciones reales, aportando así información más específica y de mayor valor cualitativo.

Tabla 5.

Volumen de ingesta de logs por tabla en Microsoft Sentinel (GB)

Table	IngestedGB
ThreatIntelIndicators	1.54
Syslog	0.77
CowrieLogs_CL	0.12

Finalmente, la combinación de estas fuentes fortalece el enfoque de detección proactiva propuesto en el estudio, permitiendo no solo registrar eventos, sino también anticipar posibles amenazas mediante el análisis integral de la información. De esta manera, se demuestra que la integración del honeypot con el SIEM no solo incrementa la visibilidad del entorno, sino que mejora significativamente la capacidad de análisis y respuesta frente a incidentes de ciberseguridad.

4.1.2. Análisis de resultados de detección por nivel de riesgo

En la Ilustración 49 se presenta la clasificación de 707 direcciones IP únicas detectadas durante el desarrollo, categorizadas según su nivel de riesgo (RiskLevel) y su coincidencia con fuentes de inteligencia de amenazas (TI_Match).

Se observa que la mayor parte de las direcciones IP se concentra en los niveles CRITICAL (335) y HIGH (302) con coincidencia en inteligencia (TI_MATCH = YES), lo que evidencia una alta proporción de actividad potencialmente maliciosa previamente identificada en fuentes externas.

Por otro lado, las categorías INFO (49), LOW (14) y MEDIUM (6) corresponden en su mayoría a direcciones IP que no presentan coincidencia con inteligencia de amenazas (TI_MATCH=NO), lo cual indica que estas detecciones fueron identificadas directamente por

el honeypot y no por Defender Threat Intelligence, aportando valor en la detección de amenazas no catalogadas previamente. Asimismo, se identifica un caso mínimo de riesgo HIGH (1) sin coincidencia, lo que podría representar una amenaza emergente no detectada por fuentes de Microsoft.

En conjunto, estos resultados demuestran la efectividad del modelo implementado, evidenciando la complementariedad entre la inteligencia de amenazas integrada en Microsoft Sentinel y los eventos capturados por el honeypot. Esta combinación permite no solo validar amenazas conocidas, sino también descubrir nuevas actividades sospechosas, fortaleciendo el enfoque de detección proactiva propuesto en la investigación.

Figura 51.

Clasificación de direcciones IP por nivel de riesgo y coincidencia con inteligencia de amenazas

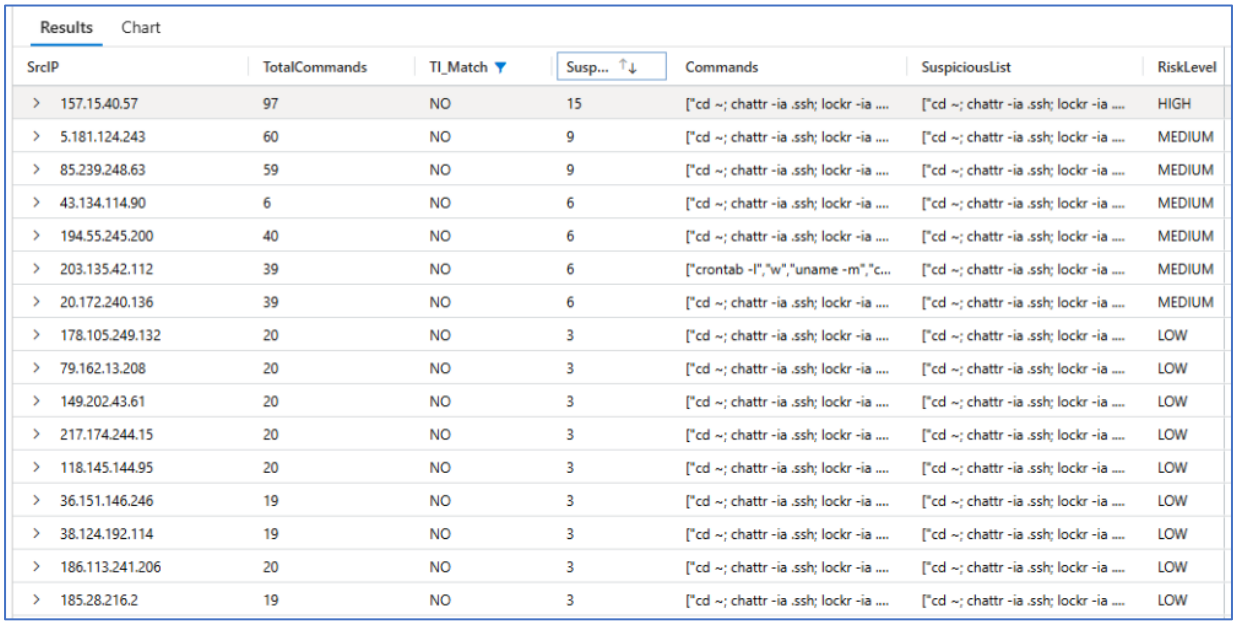
RiskLevel	TI_Match	count_
HIGH	YES	302
CRITICAL	YES	335
INFO	NO	49
LOW	NO	14
MEDIUM	NO	6
HIGH	NO	1

4.1.3. Análisis de Resultados de Comandos e IPs.

En la siguiente ilustración, se indica los resultados obtenidos de la consulta KQL construida con el fin de validar cuales son las ips, comandos y riesgo de las Ips encontradas, para esto se tienen en cuenta las consideraciones de la Tabla 1 en la construcción de la consulta, de donde se obtuvieron diversos resultados los cuales se resumirán en la Tabla

Figura 52.

Resultados de consulta KQL para clasificación de Ips por comandos



Results Chart

SrcIP	TotalCommands	TI_Match	Susp...	Commands	SuspiciousList	RiskLevel
157.15.40.57	97	NO	15	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	HIGH
5.181.124.243	60	NO	9	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	MEDIUM
85.239.248.63	59	NO	9	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	MEDIUM
43.134.114.90	6	NO	6	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	MEDIUM
194.55.245.200	40	NO	6	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	MEDIUM
203.135.42.112	39	NO	6	["crontab -l","w","uname -m","c...	["cd ~; chattr -ia .ssh; lockr -ia	MEDIUM
20.172.240.136	39	NO	6	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	MEDIUM
178.105.249.132	20	NO	3	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	LOW
79.162.13.208	20	NO	3	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	LOW
149.202.43.61	20	NO	3	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	LOW
217.174.244.15	20	NO	3	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	LOW
118.145.144.95	20	NO	3	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	LOW
36.151.146.246	19	NO	3	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	LOW
38.124.192.114	19	NO	3	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	LOW
186.113.241.206	20	NO	3	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	LOW
185.28.216.2	19	NO	3	["cd ~; chattr -ia .ssh; lockr -ia	["cd ~; chattr -ia .ssh; lockr -ia	LOW

En base a los resultados de la Ilustración 50 se procedió a resumir los comandos en el siguiente Listado de comandos más utilizados por las Ips Maliciosas:

Tabla 6.

Conteo de Comandos más utilizados por IPs Atacantes

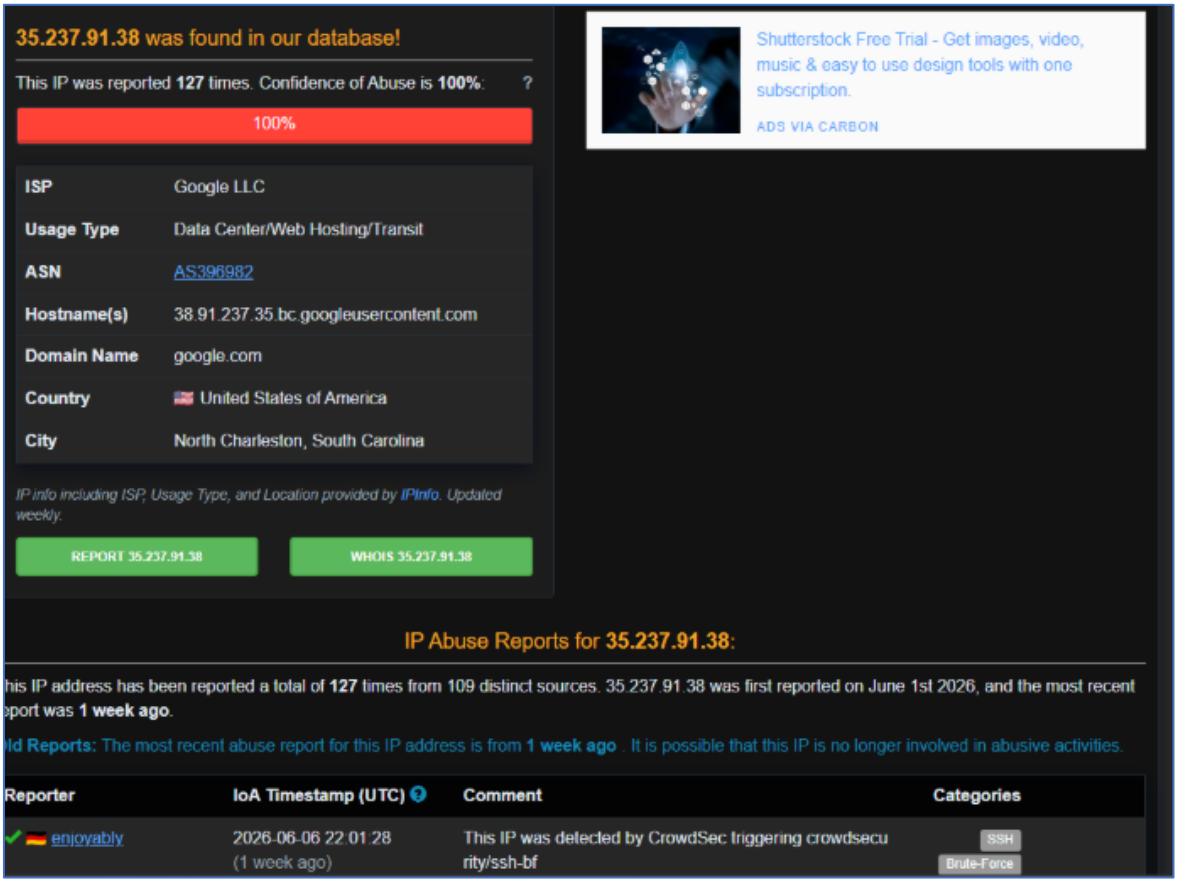
Comando	**Frecuencia**
chattr -ia .ssh	522
cd ~	480
rm -rf /tmp/auth.sh	303
pkill -9 secure.sh	303
pkill -9 auth.sh	303
echo > /etc/hosts.deny	303
pkill -9 sleep	303
ulimit -n 1020000	12
chmod 777 meow	12
./meow	12
chmod 777 meowarm64	12
./meowarm64	12
echo $(whoami):modzmodz | chpasswd	12
useradd -m -s /bin/bash admin1	12
echo admin1:modzmodz | chpasswd	12
usermod -aG sudo admin1	12

useradd -m -s /bin/bash user1	12
echo user1:modzmodz | chpasswd	12
rm -rf meow*	12
curl -O http://35.237.91.38/meowarm64	9
wget http://35.237.91.38/meowarm64	9

Se puede notar que los comandos que se observan buscan ejecutar persistencia e intentos de ejecución de malware mediante la ejecución del directorio .ssh, cambios en accesos remotos (chattr -ia .ssh), finalización de procesos con script (pkill -9 secure.sh, auth.sh, sleep), eliminación de actividad (rm -rf /tmp/auth.sh), cambios de límite de archivos abiertos (ulimit -n 1020000) con el fin de soportar una mayor carga de conexiones o descarga de ejecutables (meow y meowarm64), modificación de cuentas privilegiadas (admin1, user1), además intentos de ejecución de descargas de payload maliciosas con comandos curl o wget con la IP "35.237.91.38" la cual está asociada a actividad maliciosa de SSH y Ataque de fuerza Bruta según AbuseIPDB con 127 reportes desde el 1 de Junio del 2026, el score es de 100% de ip maliciosa y la fecha de consulta fue el 10 de Junio:

Figura 53.

Evidencia de consulta de Ip en AbuseIpDB



4.1.4. Análisis de comandos ejecutados clasificados en la Matriz MITRE

Luego de obtener el listado de comandos más utilizados, se procedió a mapear las técnicas y tácticas de MITRE asociadas a los comandos y el posible objetivo del atacante, se puede notar varios comandos que buscan realizar reconocimiento del sistema y de usuarios en una primera fase, persistencia, escalamiento de privilegios y ejecución de Malware.

Tabla 7.

Listado de Comandos con Técnicas MITRE Asociadas

Etapa del ataque	Comandos observados	Objetivo del atacante	Táctica MITRE ATT&CK	Técnica MITRE ATT&CK
Reconocimiento del sistema	Whoami	Identificar usuarios y sesiones activas	Discovery (TA0007)	T1033 – System Owner/User Discovery
Reconocimiento del sistema	uname, uname -a, uname -m, lscpu, cat /proc/cpuinfo	Determinar arquitectura y características del host	Discovery (TA0007)	T1082 – System Information Discovery
Reconocimiento del sistema	free -m, df -h, top	Evaluar recursos disponibles para ejecutar malware	Discovery (TA0007)	T1082 – System Information Discovery
Reconocimiento del sistema	crontab -l	Identificar mecanismos de persistencia existentes	Discovery (TA0007)	T1053.003 – Cron
Reconocimiento del sistema	which ls, ls -lh $(which ls)	Verificar binarios disponibles y posibles alteraciones del sistema	Discovery (TA0007)	T1083 – File and Directory Discovery
Persistencia mediante SSH	chattr -ia .ssh	Eliminar atributos que impidan modificar archivos SSH	Defense Evasion (TA0005)	T1222 – File and Directory Permissions Modification
Persistencia mediante SSH	Modificación de authorized_keys	Mantener acceso persistente mediante claves SSH	Persistence (TA0003)	T1098.004 – SSH Authorized Keys
Eliminación de competencia	pkill -9 secure.sh, pkill -9 auth.sh, pkill -9 sleep	Finalizar procesos de otros atacantes o malware	Defense Evasion (TA0005)	T1562 – Impair Defenses
Eliminación de rastros	rm -rf /tmp/auth.sh	Eliminar scripts o evidencias previas	Defense Evasion (TA0005)	T1070 – Indicator Removal on Host
Alteración de configuraciones	echo > /etc/hosts.deny	Modificar configuraciones defensivas del sistema	Defense Evasion (TA0005)	T1562 – Impair Defenses
Transferencia de malware	wget http://.../meowarm64, curl -O http://.../meowarm64	Descargar herramientas o cargas maliciosas	Command and Control (TA0011)	T1105 – Ingress Tool Transfer

Preparación para ejecución	chmod 777 meow, chmod 777 meowarm64	Asignar permisos de ejecución a los binarios descargados	Defense Evasion (TA0005)	T1222 – File and Directory Permissions Modification
Ejecución del malware	./meow, ./meowarm64	Ejecutar la carga útil en el sistema comprometido	Execution (TA0002)	T1059.004 – Command and Scripting Interpreter: Unix Shell
Creación de cuentas	useradd -m -s /bin/bash admin1, useradd -m -s /bin/bash user1	Crear nuevos usuarios persistentes	Persistence (TA0003)	T1136.001 – Create Account: Local Account
Manipulación de cuentas	echo admin1:modzmodz | chpasswd, echo user1:modzmodz | chpasswd	Establecer credenciales controladas por el atacante	Persistence (TA0003)	T1098 – Account Manipulation
Escalamiento de privilegios	usermod -aG sudo admin1	Otorgar privilegios administrativos a cuentas creadas	Privilege Escalation (TA0004)	T1098 – Account Manipulation

4.2. Análisis de Costos

Para levantar el laboratorio propuesto se debe tener en cuenta los costos asociados a la máquina virtual en la cual se desplego el Honeypot, la dirección Ip y la ingesta de Microsoft Sentinel asociada:

Tabla 8.

Detalles de Costos Azure

Service category	Service type	Region	Description	Estimated monthly cost
Compute	Virtual Machines	East US 2	1 D4s v3 (4 vCPUs, 16 GB RAM) x 730 Horas (Pay as you go), Linux, (Pay as you go); 1 managed disk – P4; Inter Region transfer type, 5 GB outbound data transfer from Este de EE. UU. 2 to Este de Asia	$144,96
Redes	IP Addresses	East US 2	Básico (clásico), 0 direcciones IP dinámicas X 730 Horas, 1 direcciones IP estáticas X 730 Horas	$2,63
			Total	**$147,59**

Aproximadamente se tendrá un costo de 150,76$ mensuales fuera del valor de la ingesta, el cual según fuentes oficiales ronda los 4,76$ por cada GB, realizando una proyección a 1 y 3 años obtenemos la siguiente tabla:

Tabla 9.

Proyección de Costos Mensual, 1 año y 3 años

Concepto	Mensual	1 Año	3 Años
Virtual Machine	$ 144,96	$ 1.739,52	$ 5.218,56
Ip Address	$ 2,63	$ 31,56	$ 94,68
TOTAL	**$ 150,76**	**$ 1.809,12**	**$ 5.427,36**

En base a estos valores tener una inversión de 150,76$ y 1809,12$ es económicamente viable para una empresa proveedora de SOC como para organizaciones que busquen mejorar su infraestructura de ciberseguridad e inteligencia de amenazas sin preocuparse por realizar mantenimientos de hardware propio, por otro lado, el costo expuesto es considerablemente menor que el de un incidente de seguridad.

Como referencia el costo anual por cada incidente de ciber seguridad en los Estados Unidos de América promedia los 4.4 millones de USD. (IBM, 2026)

Si bien existen estudios confiables que calculan el impacto económico de los incidentes de ciberseguridad en economías desarrolladas, como Estados Unidos, en Latinoamérica existe una muy poca disponibilidad de fuentes reconocidas que permitan estimar el costo promedio de un incidente de seguridad para las organizaciones de la región. Esta falta de información hace que no sea posible estimar un valor monetario al riesgo asociado a las vulnerabilidades de ciberseguridad.

4.2.1 Validación de costos reales en Microsoft Azure

Con el propósito de complementar la estimación teórica presentada mediante la calculadora de Azure, se realizó una revisión de los costos reales registrados en Azure Cost

Management durante junio de 2026. Este análisis permitió identificar el consumo efectivo de los servicios utilizados en el laboratorio, incluyendo componentes de cómputo, monitoreo, almacenamiento y red. Los resultados obtenidos proporcionan una visión más precisa del comportamiento económico de la arquitectura implementada y permiten contrastar los costos proyectados con los costos reales observados durante la ejecución del proyecto.

Tabla 10.

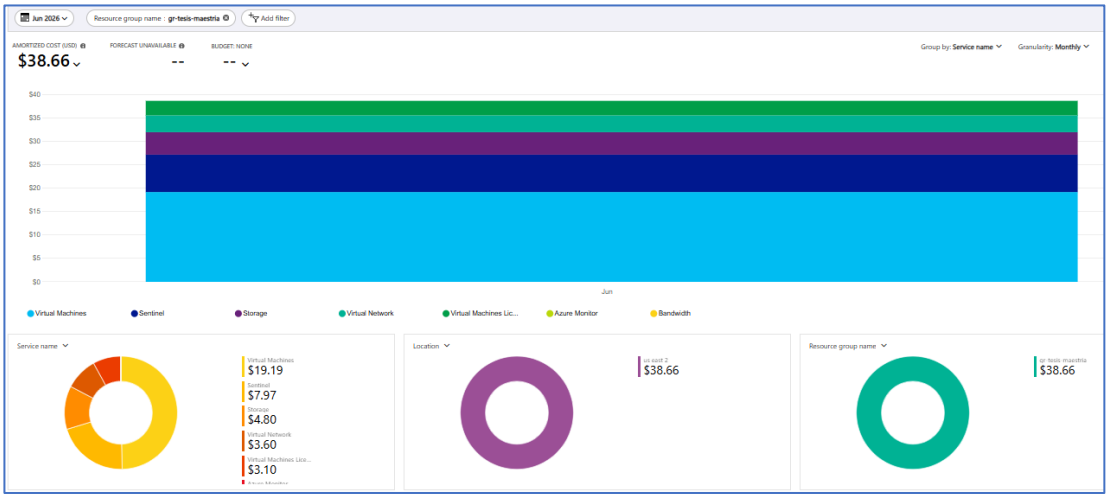
Costos reales observados en Azure durante junio de 2026

Categoría de servicio	Costo (USD)
Virtual Machines	19,19
Microsoft Sentinel	7,97
Storage	4,8
Virtual Network	3,6
Virtual Machines License	3,1
Azure Monitor	< 0,01
Bandwidth	< 0,01
TOTAL	**38,66**

Nota. Los valores corresponden al consumo registrado en Azure Cost Management para el grupo de recursos utilizado durante el desarrollo del laboratorio. El costo total observado fue de USD 38,66 durante junio de 2026. El valor efectivamente facturado por Microsoft Azure fue de USD 14,41 debido a los beneficios y créditos asociados a la suscripción utilizada con fines académicos.

Figura 54.

Análisis de costos reales por servicio en Azure Cost Management



Nota. Captura obtenida desde Azure Cost Management correspondiente al grupo de recursos GR-TESIS-MAESTRIA durante junio de 2026. Se evidencia la distribución de costos entre los principales servicios consumidos por la arquitectura implementada, incluyendo Virtual Machines, Microsoft Sentinel, Storage, Virtual Network y Azure Monitor.

La Figura 54 muestra la distribución real de costos registrada en Azure Cost Management durante junio de 2026. Se observa que el mayor componente de gasto corresponde a Virtual Machines con USD 19,19, seguido de Microsoft Sentinel con USD 7,97, Storage con USD 4,80 y Virtual Network con USD 3,60. Asimismo, se identifican costos menores asociados a licenciamiento de máquinas virtuales, Azure Monitor y tráfico de red. Estos resultados demuestran que el costo operativo de la solución no depende únicamente de la infraestructura de cómputo, sino también de los servicios de monitoreo, almacenamiento y red necesarios para la correcta operación del honeypot y su integración con Microsoft Sentinel.

CAPÍTULO 5

5. CONCLUSIONES Y RECOMENDACIONES

A continuación, se exponen las conclusiones y recomendaciones derivadas del desarrollo, implementación y evaluación de la arquitectura propuesta basada en un honeypot Cowrie integrado con Microsoft Sentinel en un entorno Microsoft Azure. Tanto las conclusiones como las recomendaciones tienen base en las pruebas realizadas, los análisis de resultados técnicos y económicos de la solución propuesta.

5.1. Conclusiones

- Se logró implementar exitosamente una arquitectura de monitoreo basada en un honeypot cowrie desplegado en Microsoft Azure e integrado con Microsoft Sentinel, validando la factibilidad técnica de utilizar servicios cloud para fortalecer las capacidades de detección temprana e inteligencia de amenazas dentro del SOC.
- La integración entre el honeypot cowrie y Microsoft Sentinel permitió visualizar eventos provenientes de múltiples fuentes de información. Los resultados combinados de estas fuentes proporcionan una visión integral del entorno monitoreado y mejoran la capacidad de análisis de seguridad.
- El sistema implementado permitió identificar y clasificar 707 direcciones IP únicas durante el periodo de observación. De estas, una proporción significativa presentó coincidencia con fuentes de inteligencia de amenazas y fue clasificada con niveles de riesgo HIGH y CRITICAL, demostrando la capacidad de la solución para detectar actividad potencialmente maliciosa y validar amenazas conocidas mediante mecanismos de correlación automatizados.
- El honeypot aportó valor adicional al proceso de detección al identificar

direcciones IP que no presentaban coincidencia con las fuentes de inteligencia de Microsoft Defender Threat Intelligence. Este resultado demuestra que la utilización de tecnologías de engaño complementa las capacidades tradicionales de inteligencia de amenazas al permitir la identificación de actividades sospechosas que aún no han sido catalogadas por fuentes externas.

- El mapeo de los eventos observados con el marco MITRE ATT&CK permitió clasificar las tácticas y técnicas empleadas por los atacantes, identificando principalmente actividades asociadas a Discovery (TA0007), Persistence (TA0003), Defense Evasion (TA0005), Privilege Escalation (TA0004), Execution (TA0002) y Command and Control (TA0011). Esto demuestra que la solución propuesta no solo detecta eventos, sino que facilita la comprensión del comportamiento adversario y fortalece las capacidades analíticas de los equipos SOC.

- La evaluación comparativa evidenció que el entorno con honeypot proporciona información de alto valor que no se encuentra disponible en entornos tradicionales. La captura de comandos ejecutados, credenciales utilizadas, direcciones IP atacantes y su posterior validación mediante plataformas de reputación permitió enriquecer significativamente el contexto de las alertas y mejorar la calidad de la información disponible para la toma de decisiones.

- Desde el punto de vista económico, la solución propuesta presenta una relación costo-beneficio favorable. La estimación inicial de la infraestructura base desplegada en Microsoft Azure proyectó un costo mensual de USD 150,76, correspondiente principalmente a la máquina virtual y la dirección IP pública. Sin embargo, el análisis de costos reales realizado durante junio de 2026

evidenció además consumo asociado a Microsoft Sentinel, almacenamiento (Storage), red (Virtual Network), monitoreo (Azure Monitor) y otros servicios complementarios necesarios para la operación de la solución. Estos resultados demuestran que el costo total de la arquitectura no depende únicamente de los recursos de cómputo, sino también de los servicios de ingesta, correlación y almacenamiento de eventos de seguridad. A pesar de estos costos adicionales, la solución continúa siendo una alternativa viable para fortalecer las capacidades de detección temprana e inteligencia de amenazas en entornos empresariales.

- Debido a que no se dispone de fuentes importantes sobre impactos de violaciones a la ciberseguridad en nuestra región podemos concluir que no es posible cuantificar el impacto económico potencial de un incidente, considerando que esto no disminuye el riesgo existente; por el contrario, incrementa la necesidad de implementar controles que permitan detectar actividades maliciosas de forma temprana y fortalecer la capacidad de respuesta ante amenazas emergentes. Por ello, la inversión anual estimada para la solución propuesta puede considerarse justificada, ya que representa un costo significativamente inferior al impacto financiero, operativo y reputacional que podría ocasionar un incidente de ciberseguridad exitoso.

5.2. Recomendaciones

- Se recomienda ampliar el periodo de monitoreo del honeypot más allá del tiempo considerado en esta investigación, con el fin de capturar una mayor cantidad de eventos, identificar tendencias de ataque a largo plazo y obtener una muestra más representativa del comportamiento de los actores maliciosos. Esta recomendación surge de los resultados obtenidos, donde se identificaron 707

direcciones IP únicas durante un periodo relativamente corto de observación.

- Se recomienda integrar fuentes adicionales de inteligencia de amenazas, tanto comerciales como de código abierto. Durante la investigación se identificaron direcciones IP detectadas por el honeypot cowrie el cual se centra en eventos de intento de ingresos por acceso remoto, es interesante repetir este laboratorio con honeypots como: Dionaea, Heralding o CitrixHoneypot por ejemplo, las cuales se centran en capturar malware, ataques de fuerza bruta y vulnerabilidades de Citrix respectivamente.
- Se recomienda automatizar la generación de indicadores de compromiso obtenidos a partir de las direcciones IP, credenciales y comandos capturados por el honeypot, permitiendo su utilización en procesos de respuesta automática y fortaleciendo las capacidades de inteligencia de amenazas de la organización.
- Se recomienda replicar la arquitectura propuesta en otros entornos cloud y escenarios empresariales con diferentes niveles de exposición a Internet, con el fin de validar la escalabilidad y adaptabilidad del modelo desarrollado. Los resultados obtenidos demuestran que la arquitectura es viable y puede servir como referencia para futuras implementaciones en SOCs.
- Se recomienda complementar futuras investigaciones con análisis estadísticos de mayor duración y con métricas de efectividad operacional, tales como tiempo medio de detección y tiempo medio de respuesta, para cuantificar de manera objetiva el impacto de los honeypots en el fortalecimiento de los procesos de monitoreo y respuesta ante incidentes.

REFERENCIAS

Al-Rubaian, A., & Al-Turjman, F. (2025). *Cloud-native SIEM architectures: Enhancing security observability in multi-cloud environments.* Retrieved from Journal of Network and Computer Applications.

Al-Zewairi, M. (2022). . *Experimental Evaluation of SIEM Systems in Detecting Modern Cyberattacks. Applied Sciences, 10(21).* Retrieved from https://doi.org/10.3390/app10217495

Behl, A. &. (2017). *Cybersecurity and cyberwar: What everyone needs to know.* Oxford University Press.

ChatGPT. (2026). *Arquitectura de un honeypot.* OpenAI.

Chen, X., & Wang, J. . (2026). *Standardizing Detection as Code: Improving MTTD and MTTR in hybrid environments.* Retrieved from Future Generation Computer Systems, 155, 120-135.

CISA., C. a. (2025). *Strategic Approach to Deception Technology in Enterprise Cloud Environments.* Retrieved from https://www.cisa.gov/resources-tools/resources/deception-technology-strategy

Cloudflare. (2026). *¿Qué es STIX/TAXII?* Retrieved from https://www.cloudflare.com/es-es/learning/security/what-is-stix-and-taxii/

Controles Empresariales. (2023). *Recopilar, detectar, investigar y responder: así funciona Microsoft Sentinel. Blog de Controles Empresariales.* Retrieved from https://blog.controlesempresariales.com/recopilar-detectar-investigar-y-responder-as%C3%AD-funciona-microsoft-sentinel

Cowrie. (2024). *Advanced SSH Honeypot for Enterprise Security*. Retrieved from https://www.cowrie.org/

CyberDefenders. (2026). *Why should SOC analysts master threat intelligence? CyberDefenders Blog.* Retrieved from https://cyberdefenders.org/blog/threat-intelligence-for-soc-analysts/

D, K. (2023). A survey of contemporary open-source honeypots, frameworks, and tools. *Journal of Network and Computer Applications*, 220.

D'souza, E. (2023). *Cloud Honeypot + SIEM Analytics: Building a Threat Detection Lab on Microsoft Azure. Medium.* Retrieved from https://medium.com/@ervindsouza08/cloud-honeypot-siem-analytics-building-a-threat-detection-lab-on-microsoft-azure-1a3bb35a6e3e

Forrester Consulting. (2024). *The Total Economic Impact™ of Microsoft Sentinel* . Retrieved from [Estudio comisionado por Microsoft]. Microsoft Security Blog.: https://www.microsoft.com/en-us/security/blog/2024/03/19/microsoft-sentinel-delivered-234-roi-according-to-new-forrester-study/

Fortinet. (2026). Retrieved from https://www.fortinet.com/lat/resources/cyberglossary/what-is-honeypot

Franco, J., et al. (2021). *A review of honeypots and honeynets for network security. IEEE Access, 9, 122811-122832.* Retrieved from https://doi.org/10.1109/ACCESS.2021.3109315

Harris, R. (2014). *Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem.* Digital Investigation.

Husari, G. (2022). *TTP-Drill: Data-Driven Threat Intelligence and Mapping to MITRE ATT&CK. Applied Sciences, 12(11).* Retrieved from https://doi.org/10.3390/app12115471

IBM . (2026). Retrieved from https://www.ibm.com/es-es/think/topics/mitre-attack

IBM. (2026). *Cost of a Data Breach Report 2025.* Retrieved from https://www.ibm.com/reports/data-breach

Kosinski, M. (n.d.). *IBM*. Retrieved from ¿Qué es la inteligencia sobre amenazas?

Microsoft . (2025). *Best practices for creating detection rules and custom analytics in Microsoft Sentinel.* Retrieved from https://learn.microsoft.com/en-us/security/operations/detect-threats-custom-analytics

Microsoft . (2026). Retrieved from https://learn.microsoft.com/es-es/kusto/query/?view=microsoft-fabric

Microsoft. (2024). *Introducción a Microsoft Sentinel. Microsoft Learn.* Retrieved from https://learn.microsoft.com/es-es/azure/sentinel/deploy-overview

Microsoft. (2026). Retrieved from https://www.microsoft.com/es-mx/security/business/security-101/what-is-a-security-operations-center-soc

Microsoft. (2026). Retrieved from https://www.microsoft.com/es-es/security/business/security-101/what-is-cyber-threat-intelligence

Microsoft. (2026). Retrieved from https://www.microsoft.com/es-es/security/business/security-101/what-is-siem#What-is-SIEM

Microsoft Tech Community. (2024). *Cowrie Honeypot and its integration with Microsoft Sentinel.* Retrieved from https://techcommunity.microsoft.com/blog/microsoftsentinelblog/cowrie-honeypot-and-its-integration-with-microsoft-sentinel-/4258349

MITRE. (2024). *ATT&CK Matrix for Enterprise*. Retrieved from https://attack.mitre.org/

MITRE Corporation . (2025). *MITRE ATT&CK®: A Framework for Adversary Emulation and Security Posture Assessment.* . Retrieved from https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_2025.pdf

MITRE Corporation. (n.d.). *MITRE ATT&CK® Enterprise Matrix.* Retrieved from https://attack.mitre.org/matrices/enterprise/

NIST . (2025). *Guide to Cyber Threat Information Sharing: Integrating Deception and Detection Mechanisms.* Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150r1.pdf

OASIS Open . (2024). *STIX/TAXII 2.1: Automated Threat Intelligence Exchange Standard.* Retrieved from https://oasis-open.github.io/cti-documentation/

Oprea, A. &. (2018). *Machine learning for cybersecurity.* IEEE Security & Privacy.

Patel, K., & Gupta, M. . (2024). *Orchestrating active defense: The role of SOAR in modern SOC operations.* Retrieved from International Journal of Information Security and Privacy, 18(2).

Sánchez-Gómez, J., et al. . (2024). *Deceptive technologies in cloud computing: A survey of honeypot integration strategies.* Retrieved from IEEE Access, 12, 58231-58250.

SANS Institute. (2026). *SANS SOC Survey.* Retrieved from https://www.sans.org/webcasts/2026-sans-soc-survey-insights

Schim, A. (2023). *ANSI*. Retrieved from https://blog.ansi.org/ansi/iso-iec-27035-1-2023-information-security-management/

SentinelOne. (2025, Agosto 19). *SentinelOne*. Retrieved from ¿Qué son los indicadores de compromiso (IoC)?: https://www.sentinelone.com/es/cybersecurity-101/threat-intelligence/what-are-indicators-of-compromise-iocs-a-comprehensive-guide/

Sikos, L. F. (2023). *AI-integrated SIEM for Intelligent Cloud Security Operations. Journal of Cloud Computing.* Retrieved from https://doi.org/10.1186/s13677-023-00412-w

Strom, B. E. (2018). *MITRE ATT&CK: Design and philosophy.* MITRE Corporation.

Torq. (2025, julio 16). Retrieved from https://torq.io/blog/mttd-vs-mttr/

Varghese, S., et al. (2024). *ntegration of Honeypots with SIEM in Cloud Environments for Real-time Threat Analysis. International Research Journal of Engineering and Technology (IRJET), 11(05).* Retrieved from https://www.irjet.net/archives/V11/i5/IRJET-V11I562.pdf

Wallarm. (2026). *Wallarm*. Retrieved from Definición de la tríada de la CIA: https://lab.wallarm.com/what/definicion-de-la-triada-de-la-cia-ejemplos-de-confidencialidad-integridad-y-disponibilidad/?lang=es

Warren Z. Cabral, C. V. (2022, 08 04). *Advanced Cowrie Configuration to Increase Honeypot.* Retrieved from https://inria.hal.science/hal-03746028v1/document

Zhang, Y., & Liu, H. . (2025). *AI-driven threat hunting: Leveraging behavioral analytics for proactive defense.* Retrieved from Cybersecurity Review, 12(1), 45-62.