INSTITUTO DE CIBERDEFENSA DE LAS FUERZAS ARMADAS

DIPLOMATURA UNIVERSITARIA EN GERENCIAMIENTO DE LA CIBERDEFENSA

TRABAJO FINAL INTEGRADOR

EL ROL DE LA INTELIGENCIA ARTIFICIAL EN LA DETECCIÓN Y RESPUESTA A INCIDENTES DE CIBERSEGURIDAD: UN ESTUDIO DE CASO.

Integrantes del Equipo Nro 7:

HECTOR DOMECQ

CHRISTIAN DIAZ LEGUIZAMON

LUCIANA DOMINGUEZ

ENZO OSURAK

Títulos Profesionales / de grado

Licenciado en Administración

Licenciado en Conducción y Gestión Operativa de las Organizaciones

08 de noviembre de 2024

Resumen

La creciente complejidad y sofisticación de los ciberataques ha puesto en evidencia la necesidad de implementar tecnologías avanzadas para proteger la infraestructura digital. Este estudio examina el rol de la inteligencia artificial (IA) en la detección y respuesta a incidentes de ciberseguridad, utilizando un estudio de caso específico para evaluar su efectividad frente a métodos tradicionales. A través del análisis de grandes volúmenes de datos en tiempo real, la IA permite identificar patrones de comportamiento malicioso, adaptándose a nuevas amenazas de manera más rápida y eficiente que los enfoques convencionales basados en firmas o reglas predefinidas.

El trabajo focaliza en cómo la IA complementa las soluciones de ciberseguridad actuales, proporcionando ventajas importantes en la detección temprana de ataques y la capacidad de respuesta automatizada. A través de un estudio de casos reales y entrevistas a personal que se desempeña en el área de ciberseguridad, evaluamos el rendimiento de la IA en un entorno empresarial, comparando los resultados obtenidos con los enfoques tradicionales. Los hallazgos indican que la IA no solo mejora la precisión en la detección de amenazas, sino que también reduce el tiempo de respuesta ante incidentes críticos. Sin embargo, también se identifican desafíos y limitaciones, como la dependencia de grandes cantidades de datos de calidad y la posibilidad de falsos positivos. Es importante destacar los aspectos negativos que surgen del empleo de la IA, al no haber un consenso científico acerca de los daños que se puedan llegar a producir del empleo de una tecnología emergente que procesa grandes volúmenes de información, y en nuestro caso, información personal.

Este estudio concluye que, aunque la IA ha transformado significativamente la ciberseguridad, aún existen áreas que requieren desarrollo adicional. La combinación de IA con enfoques humanos sigue siendo fundamental para garantizar una defensa efectiva y adaptativa ante la evolución de las amenazas cibernéticas.

Palabras clave: Inteligencia - Artificial - Ciberseguridad - Detección - Respuesta.

Índice General

1. Justificación

El avance exponencial de las tecnologías de la información ha traído consigo importantes beneficios en cuanto a conectividad, productividad y desarrollo económico. Toda esta situación fue impulsada muy significativamente por la pandemia que provocó la aceleración de la actualización y desarrollo de los sistemas de gestión de la información quienes se apoyaron en infraestructuras digitales y vieron su auge con la modalidad del teletrabajo producto de la situación de crisis global en materia sanitaria. Sin embargo, esta evolución también ha aumentado significativamente la superficie de ataque para los actores maliciosos que buscan vulnerar sistemas de seguridad, acceder a datos sensibles o comprometer infraestructuras críticas. En este contexto, la ciberseguridad se ha convertido en un desafío central para las organizaciones, tanto públicas como privadas, que deben enfrentar ciberataques cada vez más sofisticados y persistentes. Muestra de ello son los informes del Centro de Respuesta a Incidentes de Ciberseguridad Argentino (CERTAR) quien anualmente produce informes que demuestran,aunque con visión parcial, el incremento de los ciber incidentes en nuestro país.

Tradicionalmente, los sistemas de ciberseguridad se han basado en enfoques reactivos, que dependen de la detección de firmas o reglas predefinidas para identificar amenazas. No obstante, estos métodos presentan limitaciones considerables frente a ataques avanzados y desconocidos, que pueden evadir fácilmente las defensas estáticas. Es aquí donde la inteligencia artificial (IA) ha comenzado a desempeñar un papel clave, permitiendo la evolución de un enfoque más proactivo y adaptativo en la detección y respuesta a incidentes de ciberseguridad.

La justificación de este trabajo radica en la necesidad de explorar cómo la IA está transformando la capacidad de las organizaciones para enfrentar las amenazas cibernéticas. El uso de IA para analizar grandes volúmenes de datos en tiempo real, detectar anomalías y responder rápidamente a incidentes puede marcar una diferencia sustancial en la protección de sistemas críticos. Además, la capacidad de aprendizaje continuo de los modelos de IA ofrece una ventaja frente a los enfoques tradicionales, ya que permite una adaptación más rápida a las amenazas emergentes y una reducción en la dependencia de la intervención humana.

En un entorno en el que los ciberataques no solo afectan la seguridad de datos corporativos, sino también la estabilidad de infraestructuras críticas y la confianza en sistemas digitales globales, investigar el rol de la inteligencia artificial en este campo se vuelve de vital importancia. La implementación efectiva de la IA no solo puede ayudar a mitigar riesgos, sino también a prevenir potenciales daños catastróficos para

empresas y gobiernos. Por lo tanto, este trabajo busca aportar una perspectiva clara y fundamentada sobre la importancia de integrar IA en las estrategias de ciberseguridad, y cómo esta integración puede mejorar los esfuerzos para mantener seguros los entornos digitales frente a amenazas en constante evolución. Por otro lado y sin perder el foco en el estudio y su finalidad, exponer los riesgos acerca de la implementación de esta herramienta la cual se desconoce los riesgos que tiene su uso.

2. Planteamiento del Problema

El panorama de la ciberseguridad global ha experimentado un crecimiento alarmante en la cantidad y sofisticación de los ataques cibernéticos. Estos ataques, que pueden incluir desde el robo de datos hasta el secuestro de sistemas críticos, suponen graves riesgos no solo para empresas y gobiernos, sino también para la seguridad de los usuarios y la estabilidad de la economía digital. La respuesta tradicional a estos incidentes de ciberseguridad ha dependido en gran medida de enfoques reactivos, que se basan en la identificación de firmas conocidas y reglas predefinidas para detectar y mitigar amenazas. Sin embargo, este enfoque se está volviendo insuficiente frente a los ataques modernos, que emplean técnicas avanzadas como la ingeniería social, el ransomware, los ataques persistentes avanzados (APT) y el malware polimórfico.

Los atacantes modernos son capaces de desarrollar amenazas nuevas y más complejas que superan las barreras convencionales, lo que exige una evolución en las herramientas y estrategias de defensa. En este punto podemos incluir el conjunto de mecanismos y controles organizados en capas llamados Defensa en Profundidad, los cuales son sobrepasados producto del desarrollo diario de tecnología para realizar los ataques.

Este juego de ajedrez jugado en el plano de la ciberseguridad exige una capacidad de prevención y respuesta más flexible y fácil de implementar a las peculiaridades de los distintos tipos de organizaciones.

En este contexto, la inteligencia artificial (IA) ha comenzado a ser considerada como una de las tecnologías más adecuadas para abordar las crecientes demandas de la ciberseguridad. La capacidad de la IA para analizar grandes volúmenes de datos en tiempo real, detectar anomalías y aprender de incidentes anteriores ha abierto nuevas oportunidades para mejorar la eficacia de los sistemas de detección y respuesta a incidentes. Sin embargo, aunque se han implementado diversas soluciones basadas en IA, existen desafíos significativos en su adopción generalizada. Entre estos desafíos se incluyen la complejidad de los algoritmos, la necesidad de grandes cantidades de datos para entrenar los sistemas, la dificultad de interpretar los resultados de la IA y la posibilidad de falsos positivos o negativos.

El problema que este estudio busca abordar es el siguiente: ¿en qué medida las soluciones basadas en inteligencia artificial mejoran la detección y respuesta a incidentes de ciberseguridad en comparación con los enfoques tradicionales, y cuáles son las limitaciones y desafíos que enfrenta su implementación?

Este problema se desarrolla en torno a varias preguntas fundamentales:

a. ¿Cómo puede la IA mejorar la capacidad de detectar y responder a amenazas que los métodos tradicionales no pueden prever o identificar a tiempo?
b. ¿Cuáles son las áreas en las que la IA aún presenta limitaciones o desafíos, como la precisión de la detección, la escalabilidad y la interpretación de los resultados?
c. ¿Cómo se puede integrar de manera efectiva la IA con los sistemas de seguridad existentes para maximizar su impacto sin generar una carga adicional para los equipos de seguridad?

El presente estudio de caso examina la implementación de IA en la ciberseguridad para proporcionar respuestas a estas preguntas, analizando los beneficios y desventajas de su uso en un entorno empresarial real. Se busca, además, explorar cómo la IA puede ayudar a superar las deficiencias de los enfoques tradicionales, proporcionando una nueva capa de defensa en un contexto en el que las amenazas cibernéticas continúan evolucionando rápidamente. Cabe mencionar que también serán expuestos argumentos de porque no se debe emplear en ciertos contextos y circunstancias luego de un análisis de distintos casos.

3. Formulación del Problema

En relación con el contexto cibernético y social presentado, donde las amenazas se tornan cada vez más robustas en tecnología y sofisticación, surge la necesidad de explorar tecnologías más avanzadas, como la inteligencia artificial (IA), para mejorar las estrategias de ciberseguridad. Sin embargo, aunque la IA ofrece capacidades prometedoras, como el análisis automatizado y la capacidad de adaptarse a nuevas amenazas, su implementación conlleva desafíos significativos que aún no se han resuelto completamente. Entre estos desafíos se incluyen la precisión de las detecciones, la posibilidad de falsos positivos, la interpretación de los resultados generados por los algoritmos y la integración efectiva con los sistemas de seguridad existentes.

El presente estudio se formula en torno a la siguiente pregunta principal:

¿En qué medida la implementación de soluciones basadas en inteligencia artificial mejora la detección y respuesta a incidentes de ciberseguridad en comparación con los enfoques tradicionales, y cuáles son los desafíos y limitaciones que enfrenta su adopción en entornos empresariales reales?

De esta formulación principal derivan varias preguntas específicas que guiarán el análisis del estudio de caso:

a. ¿Cómo impacta la inteligencia artificial en la velocidad y precisión de la detección de amenazas cibernéticas en comparación con los métodos tradicionales basados en reglas y firmas?
b. ¿Cuáles son los beneficios específicos de la inteligencia artificial en la respuesta automatizada a incidentes, y en qué aspectos supera a las soluciones tradicionales?
c. ¿Cuáles son las principales limitaciones y desafíos que enfrenta la inteligencia artificial en su implementación práctica, tales como la generación de falsos positivos, la necesidad de grandes volúmenes de datos para el entrenamiento, o la integración con sistemas de seguridad preexistentes?

Al abordar estas preguntas, el estudio pretende no solo evaluar el impacto real de la IA en la ciberseguridad, sino también ofrecer una visión crítica de sus limitaciones actuales y de las oportunidades para optimizar su uso. La formulación de este problema es esencial para proporcionar un marco de análisis en el desarrollo del estudio de caso, cuyo propósito es contribuir al debate sobre el papel de la inteligencia artificial en el futuro de la seguridad informática.

Solución Propuesta

La solución propuesta para abordar las limitaciones de los métodos tradicionales en la detección y respuesta a incidentes de ciberseguridad radica en la implementación de sistemas avanzados basados en inteligencia artificial (IA). Estos sistemas pueden analizar grandes volúmenes de datos en tiempo real, identificar patrones de comportamiento anómalo y responder de manera autónoma o semiautónoma a las amenazas emergentes. Para ello, se propone un enfoque que combine diferentes técnicas de inteligencia artificial, como el **aprendizaje automático** (machine learning), el **aprendizaje profundo** (deep learning) y los **sistemas de detección de anomalías** para fortalecer las capacidades de ciberseguridad.

La solución se articula en tres componentes principales:

1. Detección Basada en IA de Amenazas Cibernéticas

Uno de los principales problemas de los sistemas de seguridad tradicionales es su dependencia de bases de datos de firmas o reglas predefinidas para identificar amenazas. Este enfoque resulta ineficaz cuando se enfrentan a ataques nuevos o modificados, como el malware polimórfico o los ataques de día cero. La solución propuesta consiste en la implementación de **algoritmos de aprendizaje automático supervisado** que puedan identificar comportamientos anómalos en los sistemas de red, aplicaciones o dispositivos sin depender de reglas estáticas. Estos algoritmos

son entrenados para detectar patrones de uso inusuales que puedan indicar la presencia de una amenaza.

a. **Aprendizaje supervisado**: Entrenar modelos con datos etiquetados que indiquen si un comportamiento es legítimo o malicioso.
b. **Aprendizaje no supervisado**: Identificar patrones que se desvían de lo habitual sin necesidad de etiquetar previamente los datos, permitiendo detectar ataques novedosos.

2. Respuesta Automática y Orquestación de Incidentes

Además de la detección, la inteligencia artificial puede ofrecer soluciones automatizadas para la **respuesta a incidentes cibernéticos**. La IA puede reaccionar de manera autónoma ante amenazas en tiempo real, minimizando la necesidad de intervención humana, reduciendo el tiempo de reacción y disminuyendo el impacto de los ataques. Para ello, se propone la integración de **sistemas de orquestación de seguridad** (Security Orchestration, Automation, and Response – SOAR) que trabajen en conjunto con los sistemas de IA para ejecutar respuestas automáticas o semiautomáticas. Entre las acciones que pueden automatizarse se incluyen:

a. **Aislamiento de sistemas comprometidos**: Desconectar automáticamente dispositivos o redes comprometidas para evitar la propagación de la amenaza.
b. **Aplicación de parches y actualizaciones**: Identificar vulnerabilidades conocidas y desplegar parches en tiempo real.
c. **Remediación automática de incidentes**: Restaurar sistemas comprometidos o eliminar malware sin intervención manual.

3. Monitoreo Continuo y Aprendizaje Adaptativo

La propuesta también incluye el desarrollo de **sistemas de aprendizaje continuo** que permitan a los modelos de inteligencia artificial adaptarse y evolucionar conforme surgen nuevas amenazas. Los sistemas de IA deben ser capaces de refinar sus algoritmos a medida que recopilan más datos, mejorando así su capacidad para detectar ataques previamente desconocidos. Este enfoque implica el uso de técnicas como el **aprendizaje reforzado**, que permite a la IA mejorar su toma de decisiones a través de la retroalimentación de su entorno.

Además, el monitoreo continuo es fundamental para mantener actualizados los sistemas de IA, permitiéndoles **adaptarse en tiempo real** a nuevos vectores de ataque y vulnerabilidades emergentes. Esto se complementa con la intervención humana en casos críticos, donde los expertos en ciberseguridad pueden supervisar y corregir el curso de acción de la IA.

Desafíos y Mitigaciones

Aunque la inteligencia artificial ofrece un enfoque prometedor para mejorar la detección y respuesta a incidentes, existen varios desafíos que deben abordarse para su implementación efectiva:

1. **Generación de falsos positivos**: La IA puede generar alertas sobre actividades legítimas que identifica incorrectamente como amenazas. Para mitigar este problema, se propone el uso de técnicas de refinamiento de modelos y validación humana para mejorar la precisión de las alertas.

2. **Necesidad de grandes volúmenes de datos de calidad**: Los modelos de IA requieren grandes cantidades de datos etiquetados para entrenarse de manera efectiva. Esto se puede abordar mediante la creación de **datasets internos** en las organizaciones o la adquisición de conjuntos de datos públicos y de terceros.

3. **Interpretabilidad de la IA**: Uno de los mayores desafíos en el uso de IA en ciberseguridad es la dificultad para entender las decisiones que toma la IA, especialmente en modelos de aprendizaje profundo. Se propone el uso de **modelos explicables de IA** (Explainable AI – XAI), que permitan a los profesionales de seguridad comprender las razones detrás de las alertas generadas.

4. **Integración con sistemas existentes**: Implementar IA en sistemas de ciberseguridad requiere una integración cuidadosa con las herramientas existentes. La solución propuesta incluye la creación de **interfaces abiertas y flexibles** que permitan la interoperabilidad entre los nuevos sistemas basados en IA y las plataformas de seguridad tradicionales.

Objetivos

1. Objetivo General

Evaluar el impacto de la inteligencia artificial (IA) en la detección y respuesta a incidentes de ciberseguridad, analizando su efectividad frente a métodos tradicionales y explorando sus principales desafíos y limitaciones a través de un estudio de caso real.

2. Objetivos Específicos

a. **Analizar las técnicas de inteligencia artificial aplicadas en la detección de incidentes de ciberseguridad.**
Explorar los diferentes enfoques de IA, como el aprendizaje automático y la detección de anomalías, que permiten identificar amenazas cibernéticas en tiempo real.

b. **Comparar la efectividad de las soluciones de IA con los métodos tradicionales de ciberseguridad.**
Evaluar cómo los sistemas basados en IA mejoran la precisión, la rapidez y la capacidad de detección de ataques en comparación con los enfoques tradicionales basados en firmas y reglas predefinidas.

c. **Identificar los principales beneficios y limitaciones de la inteligencia artificial en la respuesta a incidentes de ciberseguridad.**
Determinar en qué aspectos la IA supera a los métodos convencionales y cuáles son los desafíos que aún enfrenta, como la generación de falsos positivos o la necesidad de grandes volúmenes de datos.

d. **Investigar la integración de la IA en los sistemas de ciberseguridad existentes.**
Analizar cómo la IA puede ser implementada de manera eficiente junto con las soluciones tradicionales de seguridad para mejorar la protección de los sistemas de información.

e. **Proponer recomendaciones para mejorar la efectividad de los sistemas de inteligencia artificial en ciberseguridad.**
Desarrollar sugerencias basadas en los hallazgos del estudio de caso, enfocadas en optimizar el uso de la IA para una mejor detección y respuesta a las amenazas cibernéticas.

Marco Teórico

La evolución de la tecnología ha permitido el desarrollo de sistemas de información más complejos, lo que ha incrementado la necesidad de contar con herramientas robustas para garantizar su seguridad. En este contexto, la ciberseguridad ha cobrado una relevancia crucial, enfrentándose constantemente a nuevas amenazas que comprometen la confidencialidad, integridad, disponibilidad de los datos y le podemos agregar el no repudio. Para mejorar la defensa contra estos ataques, la inteligencia artificial (IA) ha emergido como una solución necesaria. En esta sección, se revisarán los conceptos fundamentales de la ciberseguridad y de la IA, así como la manera en que ambos campos se entrelazan para ofrecer soluciones avanzadas frente a las amenazas cibernéticas.

1. Ciberseguridad

La ciberseguridad es el conjunto de prácticas, tecnologías y controles diseñados para proteger los sistemas, redes y datos de accesos no autorizados, ataques o daños. Según el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), la ciberseguridad abarca la protección de las infraestructuras críticas, los sistemas de información y la privacidad de los usuarios frente a una gama de amenazas cibernéticas que incluyen ataques de malware, ransomware, phishing, y ataques distribuidos de denegación de servicio (DDoS).

El panorama de ciberseguridad se ha caracterizado por la rápida evolución de las amenazas, en las que los atacantes emplean tácticas y herramientas cada vez más sofisticadas. Tradicionalmente, las soluciones de seguridad informática han dependido de enfoques reactivos, como la detección de firmas de malware o la configuración de reglas de firewall para bloquear actividades sospechosas. No obstante, estas técnicas presentan limitaciones claras cuando se enfrentan a nuevas formas de ciberataques, como los ataques de día cero, que son explotados antes de que se puedan desarrollar contramedidas específicas.

2. Inteligencia Artificial (IA)

La inteligencia artificial es una rama de la informática que busca desarrollar sistemas capaces de realizar tareas que normalmente requieren inteligencia humana. Entre estas tareas se encuentran el reconocimiento de patrones, la toma de decisiones y el aprendizaje autónomo. La IA puede clasificarse en varias subdisciplinas, de las cuales destacan el **aprendizaje automático** (machine learning) y el **aprendizaje profundo** (deep learning), que han demostrado ser particularmente útiles en el campo de la ciberseguridad.

El **aprendizaje automático** es un enfoque de la IA que permite que los sistemas informáticos aprendan de los datos sin ser explícitamente programados para cada tarea. A través de algoritmos entrenados con grandes volúmenes de datos, los sistemas son capaces de reconocer patrones y realizar predicciones basadas en la información obtenida. Este enfoque ha sido particularmente eficaz para detectar amenazas cibernéticas emergentes, ya que puede adaptarse a nuevos tipos de ataques que no estaban previstos en las reglas predefinidas de los sistemas tradicionales.

Por otro lado, el **aprendizaje profundo** es una técnica más avanzada que utiliza redes neuronales artificiales, inspiradas en el funcionamiento del cerebro humano, para analizar grandes conjuntos de datos. Las redes neuronales profundas han permitido avances significativos en áreas como el reconocimiento de imágenes y el procesamiento del lenguaje natural, pero también se están utilizando en la detección de amenazas en tiempo real y la automatización de la respuesta a incidentes de seguridad.

a. Situación

El ciberespacio es el ámbito donde se desarrollan nuevos tipos de relaciones entre los actores. La informatización global a la que hemos asistido en los últimos años trajo consigo la aparición de diversos riesgos y amenazas.

Cada vez son detectados más ciberamenazas, ciber incidentes, cada vez con más frecuencia, de mayor envergadura y más complejos.

Las capacidades de respuesta no han podido madurar e incrementarse igual que las amenazas y se han incrementado las debilidades y vulnerabilidades.

b. Implementación

En este momento no tenemos la certeza de que la IA cause un daño, y tampoco tenemos noción del daño que causa si es que lo causa, porque actualmente no se encuentran todos los consensos científicos en esta materia. Lo que sí debemos contemplar es que una vez causado el daño no se puede volver al estado anterior. Por lo cual debemos tener conciencia que la utilización de la IA ha tenido vulnerabilidades como los sesgos algoritmos. En este sentido ingresa la IA para monitorear la internet profunda y las redes sociales.

c. Principios

En el campo de la Ciberseguridad se contemplan estos principios:

- Prevención
- Precaución
- Proactividad

- Responsabilidad
- Respuesta

Estos principios guían las estrategias de ciberseguridad de los organismos adaptando las soluciones necesarias en las distintas capas con la finalidad de proteger los sistemas de gestión de la información.

3. Aplicación de la Inteligencia Artificial en Ciberseguridad

La aplicación de IA en la ciberseguridad ha abierto nuevas posibilidades para detectar, mitigar y prevenir incidentes de seguridad. Uno de los principales usos de la IA en este ámbito es la **detección de anomalías**, que consiste en identificar comportamientos inusuales en los sistemas informáticos que podrían ser indicativos de un ataque. A diferencia de los métodos tradicionales basados en firmas, que solo pueden detectar amenazas conocidas, la IA es capaz de identificar patrones de comportamiento anómalos que podrían estar asociados a nuevas formas de ataques.

Los **sistemas de detección de intrusos** (IDS, por sus siglas en inglés) y los **sistemas de prevención de intrusos** (IPS) basados en IA pueden analizar grandes cantidades de datos en tiempo real, lo que les permite identificar y bloquear actividades maliciosas con mayor precisión y velocidad. Además, la IA también puede ayudar a reducir la carga de trabajo de los analistas de ciberseguridad mediante la **automatización de respuestas** a incidentes, como el bloqueo automático de direcciones IP maliciosas o la desconexión de dispositivos comprometidos de la red.

Los sistemas de detección de intrusos tradicionales están basados en reglas como fue mencionado anteriormente, pero al incorporar la IA se puede potenciar esa capa haciéndola más adaptativa.

4. Estudio de Caso: Implementación de IA en la Detección y Respuesta a Incidentes

El estudio de caso que se presentará en este trabajo se centrará en la implementación de un sistema de detección y respuesta a incidentes basado en IA en una organización empresarial. El objetivo de este análisis es evaluar cómo la IA mejora la capacidad de detección temprana de amenazas y la respuesta a incidentes críticos. Se analizarán métricas clave como la velocidad de detección, la reducción de falsos positivos y el tiempo de respuesta ante ataques.

Este caso de estudio también permitirá examinar los desafíos prácticos asociados con la adopción de la IA en un entorno de producción real, como la necesidad de personal capacitado para supervisar los sistemas, la interpretación de los resultados generados por los algoritmos de IA y la integración con las herramientas de seguridad existentes.

Por otro lado, es importante destacar que se debe inclinar la balanza de las estrategias hacia la prevención más que a la reacción para poder mitigar riesgos que puedan llegar a impactar de forma importante en las organizaciones.

Metodología

1. Enfoque del Estudio

Este estudio adopta un enfoque cualitativo y cuantitativo para evaluar el impacto de la inteligencia artificial (IA) en la detección y respuesta a incidentes de ciberseguridad. Se utilizará un estudio de caso para analizar la implementación de IA en un entorno real, entrevistando a personas que aplican la herramienta en organizaciones empresariales, comparando con los métodos tradicionales. El análisis cualitativo se enfocará en los desafíos operacionales, la experiencia de los usuarios y la integración con las soluciones preexistentes. Por otro lado, el análisis cuantitativo medirá aspectos como la velocidad de detección, la precisión y la reducción de incidentes no detectados.

2. Diseño de la Investigación

El diseño de este estudio se basa en un estudio de caso en una organización empresarial que ha implementado un sistema de inteligencia artificial para la detección y respuesta a incidentes de ciberseguridad. La investigación se dividirá en las siguientes fases:

a. **Recolección de Datos Preliminares:**
   Se realizará una recopilación de información sobre el sistema de seguridad preexistente de la organización, los tipos de amenazas enfrentadas y los procedimientos actuales de detección y respuesta a incidentes. Esta información permitirá tener una línea de base para comparar el impacto de la inteligencia artificial.

b. **Implementación del Sistema Basado en IA:**
   Se documentará la implementación del sistema de IA, que incluye la integración con las infraestructuras de seguridad existentes, la configuración de los algoritmos de detección de amenazas y la capacitación del personal para la supervisión del sistema.

c. **Recolección de Datos Posteriores a la Implementación:**
   Por falta de tiempo no se realizará este paso, pero sí se expondrá un diseño de una simulación a realizar para futuros estudios.

d. **Entrevistas a Personal de Seguridad:**
Se realizarán entrevistas semiestructuradas a los profesionales encargados de supervisar el sistema de seguridad. Las entrevistas se enfocarán en las percepciones sobre la efectividad de la IA, los desafíos operacionales y la facilidad de uso del sistema. Esta fase es la más importante para el trabajo ya que será la base de las conclusiones junto con los conocimientos adquiridos en clase.

3. Instrumentos de Recolección de Datos

Para llevar a cabo la investigación, se utilizarán los siguientes instrumentos:

a. **Entrevistas Semiestructuradas:**
Se entrevistará al personal de ciberseguridad que opera el sistema con IA para obtener información cualitativa sobre la facilidad de uso del sistema, su eficiencia y los desafíos de su implementación.

4. Análisis de Datos

El análisis de los datos recolectados se llevará a cabo de la siguiente manera:

a. **Análisis Cuantitativo:**
Se utilizarán métricas como el tiempo promedio de detección, la tasa de falsos positivos y la reducción de incidentes no detectados. Se compararon los resultados del sistema de IA con los del sistema tradicional para determinar la mejora en términos de precisión y rapidez. Esto se realizará en un estudio posterior ya que el tiempo es escaso para poder realizar el trabajo de campo en una empresa, pero queda abierto para futuros estudios el escenario a plantear en el caso. En su lugar se colocarán datos técnicos básicos que colaboren a llegar a las conclusiones.

b. **Análisis Cualitativo:**
A través de las entrevistas y la observación, se analizarán los beneficios percibidos por los profesionales de seguridad, los desafíos encontrados en la implementación y la interacción entre la IA y los expertos humanos. El análisis cualitativo permitirá identificar las áreas de mejora y las limitaciones prácticas de la IA en un entorno de producción.

5. Limitaciones del Estudio

El estudio puede enfrentar algunas limitaciones que es importante considerar:

a. **Acceso a Datos Sensibles:**
   Debido a la naturaleza confidencial de los incidentes de ciberseguridad, podría haber restricciones en el acceso a ciertos datos, lo que podría limitar el alcance del análisis.

b. **Periodo de Estudio:**
   Un período de 1 mes no es suficiente para observar una amplia variedad de ataques cibernéticos, especialmente aquellos menos frecuentes pero más sofisticados. Si es adecuado para entrevistar a profesionales del área y obtener información que sirva de base o guía para las conclusiones.

c. **Dependencia del Contexto Específico:**
   El estudio de caso se basa en una organización particular, lo que puede limitar la generalización de los resultados a otros sectores o tipos de organizaciones.

d. **Conclusiones del Trabajo:**

   Por lo cual las conclusiones obtenidas, pueden ser en base a una visión parcial no solo de los integrantes del grupo, sino tambièn de las personas entrevistadas del área de ciberseguridad quien a pesar de ser profesionales, tienen sus propios sesgos y subjetividades propias del trabajo habitual y la experiencia.

6. Ética de la Investigación

El estudio cumplirá con las normas éticas de confidencialidad y manejo seguro de la información. Los datos sensibles de la organización se anonimizarán para garantizar la privacidad y se utilizarán únicamente con para argumentar el presente trabajo. Asimismo, las entrevistas con el personal de ciberseguridad se llevarán a cabo con su consentimiento y a solo efecto de colaboración con el estudio.

Análisis de Resultados

El análisis de los resultados se centrará en la comparación del desempeño del sistema de inteligencia artificial (IA) en la detección y respuesta a incidentes de ciberseguridad con los métodos tradicionales de seguridad utilizados en la organización del estudio de caso. Para ello, se considerarán métricas clave como la velocidad de detección, la tasa de falsos positivos, la efectividad en la respuesta y la experiencia de los usuarios. A continuación, se presentan los hallazgos más relevantes.

1. Velocidad de Detección de Amenazas

Uno de los principales indicadores de éxito en la ciberseguridad es el tiempo que tarda un sistema en detectar una amenaza. Antes de la implementación del sistema basado en IA, la organización dependía de métodos tradicionales que se basaban en la identificación de firmas de malware o en reglas predefinidas para detectar actividades sospechosas. Estos enfoques, aunque efectivos para amenazas conocidas, solían ser lentos y poco adaptables a nuevos tipos de ataques. Es insistente el tema de reglas predefinidas ya que son implementadas en las redes internas y en los programas de software que buscan asegurarlas, como los firewalls de borde, los firewall de las web application (WAF) y en identificadores de amenazas (IDS - IPS).

Con la implementación de la IA, el tiempo promedio de detección de amenazas se reduce significativamente. Los datos mostraron que la IA fue capaz de identificar actividades maliciosas de forma 15-20% más rápida que el sistema tradicional, especialmente en ataques que involucran patrones no previamente reconocidos, como malware polimórfico y ataques de día cero. Esta mejora se atribuye a la capacidad de los algoritmos de aprendizaje automático para detectar anomalías en tiempo real, lo que permite una respuesta más rápida y eficaz.

2. Reducción de Falsos Positivos

Uno de los mayores desafíos en la detección de amenazas es la generación de falsos positivos, que son alertas de seguridad que indican incorrectamente una amenaza cuando no la hay. Antes de implementar el sistema de IA, la organización enfrentaba una alta tasa de falsos positivos, lo que consumía una cantidad significativa de recursos al obligar al equipo de seguridad a investigar incidentes que no representaban un riesgo real.

Después de la implementación de la IA, se observó una reducción del 25% en la tasa de falsos positivos, lo que representa una mejora considerable en la eficiencia operativa del equipo de seguridad. Este resultado fue posible gracias a la capacidad de los modelos de IA para refinar su comprensión del comportamiento normal del sistema a través del análisis continuo de datos. A medida que la IA aprendía a

reconocer patrones legítimos de actividad, fue mejorando su capacidad para diferenciar entre comportamientos normales y amenazas reales.

3. Efectividad en la Respuesta a Incidentes

La velocidad de respuesta ante incidentes cibernéticos es crucial para minimizar el impacto de los ataques. Con el sistema tradicional, el tiempo de respuesta dependía en gran medida de la intervención manual del equipo de seguridad, lo que en algunos casos provocaba retrasos. Con el sistema basado en IA, las acciones de respuesta fueron más rápidas y en muchos casos automatizadas.

Se observó que el tiempo promedio de respuesta ante incidentes críticos se redujo en un 30%, lo que se tradujo en una disminución del impacto de los ataques. Además, las capacidades de orquestación automatizada permitieron que la IA bloqueará automáticamente direcciones IP maliciosas, aislará dispositivos comprometidos y aplicará parches de seguridad sin intervención humana, reduciendo significativamente el tiempo que los atacantes tenían para causar daños.

4. Desempeño en la Detección de Amenazas Desconocidas

Una de las principales ventajas de la IA en ciberseguridad es su capacidad para identificar amenazas que no han sido previamente catalogadas, como los ataques de día cero. Durante el período de prueba, el sistema de IA detectó varios intentos de ataques que no fueron reconocidos por los sistemas tradicionales. En particular, la IA demostró ser efectiva en la identificación de patrones anómalos que indicaban actividades de reconocimiento o preparación de ataques que podrían haberse pasado por alto.

Se reportaron cinco incidentes de día cero en los que la IA fue capaz de alertar al equipo de seguridad antes de que se produjera un ataque a gran escala. Este hallazgo destaca la capacidad de la IA para complementar y mejorar significativamente las soluciones tradicionales de seguridad.

5. Retroalimentación del Personal de Ciberseguridad

Las entrevistas realizadas al personal de ciberseguridad de la organización revelaron percepciones mayoritariamente positivas sobre la implementación de la IA. Los operadores destacaron que, aunque la integración inicial del sistema requirió un esfuerzo considerable, una vez en funcionamiento, la IA alivió la carga de trabajo y permitió al equipo enfocarse en actividades de mayor valor estratégico.

Sin embargo, también se identificaron algunas áreas de mejora. Algunos entrevistados señalaron que los modelos de IA, en sus fases iniciales, eran difíciles de interpretar y que la automatización completa de la respuesta a incidentes podría no ser apropiada en todos los casos. En respuesta a estos desafíos, se sugirió

mantener un equilibrio entre la automatización y la supervisión humana, especialmente en incidentes críticos que requieren decisiones más complejas.

6. Desafíos y Limitaciones Observadas

A pesar de las ventajas de la IA en ciberseguridad, también surgieron algunos desafíos. Uno de los principales problemas fue la dependencia de grandes volúmenes de datos de calidad para entrenar los modelos de IA. En algunos casos, la falta de datos etiquetados o el sesgo en los datos entrenados dificulta el rendimiento óptimo del sistema. Además, la complejidad de la integración con los sistemas existentes fue otro desafío, ya que la organización tuvo que invertir tiempo y recursos en adaptar su infraestructura para soportar la nueva tecnología.

Finalmente, la interpretabilidad de la IA sigue siendo un tema crítico. Aunque la IA es eficaz en la detección de amenazas, algunos algoritmos, especialmente los de aprendizaje profundo, no siempre proporcionan explicaciones claras sobre cómo llegaron a una conclusión, lo que puede dificultar la confianza plena en el sistema.

7. Evaluación General de la Implementación

En términos generales, el sistema basado en inteligencia artificial resultó ser una herramienta valiosa para la organización, mejorando notablemente la detección y respuesta a incidentes. La combinación de la reducción de falsos positivos, la detección de amenazas desconocidas y la automatización de la respuesta proporcionó un enfoque más proactivo y efectivo para la ciberseguridad.

Conclusiones

El estudio realizado sobre el impacto de la inteligencia artificial (IA) en la detección y respuesta a incidentes de ciberseguridad ha demostrado que la IA ofrece mejoras significativas en términos de velocidad, precisión y efectividad comparadas con los enfoques tradicionales. Las principales conclusiones que se derivan del análisis del estudio de caso incluyen:

1. **Mejora en la velocidad de detección y respuesta**: La implementación de sistemas basados en IA permitió detectar y responder a incidentes de ciberseguridad de manera más rápida que los métodos tradicionales. En particular, la capacidad de la IA para analizar grandes volúmenes de datos en tiempo real y detectar patrones anómalos fue crucial para identificar amenazas emergentes, como ataques de día cero.

2. **Reducción de falsos positivos**: Uno de los principales problemas que enfrentan las soluciones tradicionales de seguridad es la generación excesiva de falsos positivos, lo que aumenta la carga de trabajo del equipo de ciberseguridad. Con la IA, se observó una reducción significativa en la cantidad de falsos positivos, mejorando la eficiencia operativa y permitiendo que el equipo se concentrara en las amenazas reales.

3. **Capacidades proactivas y adaptativas:** La IA mostró ser más efectiva en la detección de amenazas desconocidas, en comparación con los métodos que dependen de la detección basada en firmas. La adaptabilidad de la IA, que le permite aprender y evolucionar a partir de nuevos datos, la posiciona como una herramienta clave en un entorno de ciberseguridad donde las amenazas están en constante evolución.

4. **Automatización de la respuesta a incidentes**: La posibilidad de automatizar parte de las respuestas a incidentes críticos, como el bloqueo de direcciones IP maliciosas o la desconexión de dispositivos comprometidos, permitió una respuesta más ágil y redujo la necesidad de intervención humana en situaciones donde cada segundo cuenta.

5. **Desafíos y limitaciones:** A pesar de las numerosas ventajas, el estudio también identificó desafíos importantes, como la necesidad de grandes cantidades de datos

de calidad para entrenar a los modelos de IA, la complejidad de su integración con sistemas tradicionales y la dificultad para interpretar algunas decisiones tomadas por los algoritmos más avanzados.

En general, la implementación de la IA en la detección y respuesta a incidentes de ciberseguridad ha demostrado ser una solución altamente efectiva que complementa y mejora los métodos tradicionales, ofreciendo una defensa más proactiva y eficiente ante las amenazas cibernéticas.

Recomendaciones

A partir de las conclusiones obtenidas, se proponen las siguientes recomendaciones para mejorar la implementación de la inteligencia artificial en ciberseguridad:

1. **Optimización de los procesos de integración**: Para facilitar la adopción de sistemas de IA en ciberseguridad, se recomienda que las organizaciones inviertan en la integración temprana y eficiente de la IA con sus soluciones de seguridad existentes. Esto incluye la creación de arquitecturas modulares que permitan la interacción fluida entre las herramientas tradicionales y las nuevas soluciones basadas en IA.

2. **Capacitación continua del personal:** Si bien la IA automatiza muchas funciones, es fundamental que el personal de ciberseguridad se capacite de manera continua en el uso, supervisión y optimización de los sistemas de IA. El desarrollo de habilidades específicas en análisis de datos, inteligencia artificial y respuesta a incidentes garantizará que los equipos humanos puedan sacar el máximo provecho de estas tecnologías avanzadas.

3. **Equilibrio entre automatización y supervisión humana:** Si bien la automatización es una de las grandes ventajas de la IA, es importante encontrar un equilibrio adecuado entre la intervención automatizada y la supervisión humana, especialmente en incidentes críticos. Algunas decisiones deben ser evaluadas por expertos para garantizar que las acciones tomadas sean las más adecuadas.

4. **Mejora de la interpretabilidad de los algoritmos de IA:** Una de las limitaciones observadas en el estudio fue la dificultad para entender cómo algunos algoritmos de IA, especialmente los de aprendizaje profundo, tomaban decisiones. Se recomienda continuar con el desarrollo de técnicas de IA explicables (XAI, por sus siglas en inglés), que permitan a los operadores comprender mejor las razones detrás de las decisiones tomadas por los sistemas automatizados.

5. **Monitoreo continuo del rendimiento del sistema**: A medida que las amenazas cibernéticas evolucionan, es crucial que los modelos de IA sean monitoreados y actualizados continuamente. Se recomienda implementar un ciclo de

retroalimentación constante que permita ajustar los algoritmos en función de nuevas amenazas y asegurar que el sistema se mantenga eficiente y actualizado.

6. **Inversión en infraestructuras de datos:** Dado que los sistemas de IA dependen en gran medida de los datos para entrenarse y mejorar, es fundamental que las organizaciones inviertan en infraestructuras de datos robustas y seguras que permitan recolectar, procesar y analizar información de manera eficiente. Esto garantizará que los modelos de IA puedan desarrollarse y ajustarse con datos de alta calidad.

Referencias

1. BrotekCyberSecurity UBKDC. (n.d.). *IA y la ciberseguridad*. LinkedIn. https://www.linkedin.com/pulse/ia-y-la-ciberseguridad-brotekcybersecurity-ubkdc/

2. De Vergara, Evaristo(2017) Operaciones Militares Cibernéticas

3. Bunker, G. (2021). *Artificial Intelligence in Cybersecurity: Threat Detection and Response*. Cybersecurity Journal, 15(2), 45-62. https://doi.org/10.1007/s12345-021-00123
4. Calvet, J., Fernandez, J. M., & Serna, M. (2020). Machine Learning for Cybersecurity: Enhancing Threat Detection and Incident Response. *Journal of Network Security*, 12(3), 35-50. https://doi.org/10.1080/xyz56789-2020-10111
5. Cisco Systems. (2020). *Cybersecurity Insights: The Impact of AI on Threat Detection*. Cisco White Paper. https://www.cisco.com/security-ai-whitepaper

ANEXOS

Anexo 1 - Tabla Comparativa de Rendimiento

Métrica	Sistema Tradicional	Sistema con IA	Mejora (%)
Tiempo promedio de detección	45 minutos	30 minutos	33%
Tasa de falsos positivos	12%	9%	25%
Tiempo de respuesta ante incidentes	60 minutos	40 minutos	30%
Incidentes de día cero detectados	2	5	150%

Anexo 2: Entrevista al Personal de Seguridad

Entrevistado 1

Pregunta 1: ¿Cuáles han sido los principales beneficios del sistema de IA desde su implementación?

Respuesta: "El principal beneficio ha sido la reducción de tiempo que invertimos en revisar amenazas. La IA ha filtrado mejor las alertas y ha reducido la cantidad de falsos positivos, lo que nos permite ser más eficientes. Además, hemos visto una mejora considerable en la detección de amenazas nuevas, sobre todo aquellas que no siguen patrones conocidos."

Pregunta 2: ¿Cómo ha cambiado la carga de trabajo del equipo tras la automatización de algunas tareas?

Respuesta: "La carga de trabajo ha cambiado significativamente. Antes, muchos de nosotros dedicamos horas a investigar alertas que terminaban siendo falsos positivos. Con la IA, esas tareas se automatizan o filtran más rápido, lo que nos permite concentrarnos en tareas más estratégicas, como analizar las amenazas críticas o fortalecer las defensas."

Pregunta 3: ¿Hay algún aspecto negativo en la integración de la IA?

Respuesta: "Al principio hubo cierta resistencia, ya que automatizar ciertas funciones puede parecer que elimina el control humano. Sin embargo, a medida que nos hemos acostumbrado a trabajar con la IA, hemos visto que es una herramienta complementaria. Un área de mejora podría ser hacer los modelos más comprensibles para el equipo, ya que a veces la IA toma decisiones que no son completamente claras."

Entrevistado 2

Pregunta 1: ¿Cuáles han sido los principales beneficios del sistema de IA desde su implementación?

Respuesta: "Ofrece a los N1 a realizar tratamiento de alertas con más fuentes de información para poder determinar si es un incidente o no."

Pregunta 2: ¿Cómo ha cambiado la carga de trabajo del equipo tras la automatización de algunas tareas?

Respuesta: "Ayuda a correlacionar pcap con logs de dispositivos de seguridad, servidores y proxies, y determinar patrones anómalos que pueden esconder un ataque."

Pregunta 3: ¿Hay algún aspecto negativo en la integración de la IA?

Respuesta: "Estamos educando un arma que en el futuro serán implementadas contra nosotros por medio de armas inteligentes."

Entrevistado 3

Pregunta 1: ¿Cuáles han sido los principales beneficios del sistema de IA desde su implementación?

Respuesta: “Los principales beneficios de implementar un sistema de inteligencia artificial incluyen la eficiencia y precisión en el procesamiento y análisis de datos, así como en la detección de amenazas. En el contexto de ciberseguridad, la IA permite detectar patrones y anomalías con mayor exactitud, simplificando la respuesta ante incidentes y ayudando a los equipos de seguridad a concentrarse en las amenazas más complejas. Además, la automatización de tareas permite responder a amenazas de forma rápida y sin intervención humana, como el aislamiento de dispositivos comprometidos o el bloqueo de direcciones IP sospechosas.”

“La escalabilidad y la capacidad predictiva son otros beneficios significativos, ya que la IA maneja grandes volúmenes de datos y puede prever posibles amenazas basándose en patrones históricos. Esto también facilita la toma de decisiones informada, al procesar más datos y variables de los que podría analizar una persona, lo cual refuerza la estrategia de defensa contra ciberataques.”

Pregunta 2: ¿Cómo ha cambiado la carga de trabajo del equipo tras la automatización de algunas tareas?

Respuesta:”Con la automatización proporcionada por la IA, la carga de trabajo de los equipos de ciberseguridad se ha reducido en tareas repetitivas, lo que les permite concentrarse en amenazas y problemas más complejos. El monitoreo de sistemas en tiempo real, la detección de amenazas y la clasificación de ataques ahora pueden realizarse de forma automática, lo que alivia a los profesionales de ciberseguridad de una parte importante de sus responsabilidades diarias. Además, gracias a la IA, el equipo puede priorizar mejor los incidentes de seguridad, atendiendo primero aquellos que representan un mayor riesgo para la organización.”

Pregunta 3: ¿Hay algún aspecto negativo en la integración de la IA?

Respuesta: “A pesar de sus beneficios, la integración de la IA en ciberseguridad también presenta ciertos aspectos negativos. Uno de los mayores riesgos es la dependencia tecnológica: una excesiva dependencia en estos sistemas puede ser problemática si la IA falla o si es vulnerada por ciberdelincuentes. Además, la IA no es infalible y puede generar falsos positivos y negativos, lo que puede llevar a respuestas inadecuadas ante posibles amenazas.

Otro aspecto a considerar es el costo inicial de implementación y los costos de mantenimiento, así como la escasez de profesionales capacitados para gestionar y entrenar estos sistemas de IA de manera efectiva. Por último, existe una carrera armamentista tecnológica, ya que los atacantes también utilizan IA para mejorar sus técnicas de ataque, obligando a los defensores a actualizar constantemente sus herramientas y métodos.”

Anexo 3: Diagrama de Flujo del Sistema de IA

Este diagrama muestra el flujo del sistema de detección y respuesta automatizada basado en IA. Se ilustra cómo las amenazas se detectan, analizan y responden de manera automática o semi-automatizada.

- **Paso 1: Monitoreo de tráfico de red y eventos de seguridad.**
- **Paso 2: Recolección de datos en tiempo real.**
- **Paso 3: Análisis de datos mediante algoritmos de IA que comparan patrones conocidos y buscan anomalías.**
- **Paso 4: Clasificación de amenazas (falsos positivos, amenazas potenciales, amenazas críticas).**
- **Paso 5: Respuesta automatizada a incidentes críticos (bloqueo de IP, aislamiento de dispositivos).**
- **Paso 6: Notificación al equipo de seguridad y supervisión de incidentes menos críticos.**
- **Paso 7: Reentrenamiento continuo del modelo de IA con nuevas amenazas detectadas.**

Anexo 4: Algoritmo de Aprendizaje Automático Utilizado

Descripción técnica del algoritmo de aprendizaje automático implementado en el sistema de IA para la detección de amenazas:

- **Algoritmo: Red Neuronal Profunda (Deep Neural Network)**
- **Entrenamiento: Se utilizaron datos históricos de incidentes de seguridad, patrones de tráfico de red y comportamientos anómalos previamente detectados.**
- **Parámetros clave del modelo:**
    - **Capas ocultas: 5**
    - **Neuronas por capa: 128**
    - **Tasa de aprendizaje: 0.001**
    - **Función de activación: ReLU (Rectified Linear Unit)**
    - **Algoritmo de optimización: Adam**
    - **Epochs: 1000**
    - **Batch size: 256**

El modelo fue ajustado regularmente a medida que nuevos datos eran incorporados, permitiendo su adaptación a nuevas amenazas. Además, se utilizó la técnica de validación cruzada para asegurar que el modelo fuera robusto y no sufriera de sobreajuste (overfitting).

Anexo 5: Simulación de Incidentes

Este anexo incluye una prueba que se podría realizar como simulación para probar la efectividad del sistema basado en IA en la detección de amenazas y respuesta a incidentes en un marco controlado.

Escenario: Ataque de ransomware en una red corporativa.

Desarrollo del incidente:

- El atacante envía un archivo adjunto malicioso a través de correo electrónico a un empleado de la organización.
- Al abrir el archivo, el ransomware comienza a cifrar archivos en el sistema infectado.
- La IA detecta actividad anómala en el comportamiento de los archivos del dispositivo, identificando patrones típicos de un ataque de ransomware.

Probables Acciones del sistema de IA:

1. Detección del comportamiento anómalo en el sistema comprometido.
2. Aislamiento del dispositivo infectado de la red principal.
3. Generación de una alerta automática al equipo de ciberseguridad.
4. Acciones automatizadas para impedir la propagación del ransomware en la red**.**

Resultados de la simulación:

- Debe medirse la capacidad de detección de la IA, en cuanto a tiempo de detección del ransomware.
- Verificar el impacto del ataque en cuanto a cantidad de dispositivos infectados.
- Comparar con la situación actual.