Intracom Journal

Análisis de herramientas de Inteligencia Artificial en la detección de ciberamenazas en tiempo real en el sector educativo

Analysis of Artificial Intelligence tools in the Detection of cyber threats in Real Time in the educational sector

Camilo Augusto Cardona Patiño
Fundación Universitaria del Área Andina
cccardona19@areandina.edu.co
https://orcid.org/0000-0001-8758-6603

Helber Leandro Báez Rodríguez
Fundación Universitaria del Área Andina
https://orcid.org/0000-0002-7551-5530

Gustavo Enrique Tabares Parra
Fundación Universitaria del Área Andina
https://orcid.org/0000-0003-1275-0346

Claudia Patricia Ramírez Triana
Fundación Universitaria del Área Andina
https://orcid.org/0000-0003-1044-090X

https://doi.org/10.61283/hyqney43

Recepción: 17.10.2024 Aceptación: 02.11.2024 Publicación: 31.12.24

ABSTRACT

In a changing educational environment, participatory The current proposal investigated the integration of cybersecurity tools based on artificial intelligence (AI) in the educational context. The objective set was to identify the most effective technologies for protecting sensitive information in educational institutions. For the development, a qualitative methodology was employed, involving an exhaustive exploration of literature related to key trends and tools. Subsequently, a comparative analysis of these tools was conducted based on their effectiveness, adaptability, and ease of implementation. The results obtained demonstrated that AI has the potential to detect and respond quickly to potential threats, which optimizes the management of cybersecurity through task automation processes while promoting a stronger security culture among students and employees. It was concluded that the adoption of the evaluated technologies helps to strengthen computer security, while improving resource management, promoting a safe and resilient educational environment.

KEYWORDS: education; Cybersecurity; artificial intelligence; security tools; data protection; security automation

RESUMEN

En la actual propuesta se indaga acerca de la integración de herramientas de ciberseguridad basadas en inteligencia artificial (IA) en el contexto educativo. El objetivo planteado fue el de reconocer las tecnologías más efectivas para la protección de la información sensible en instituciones educativas. Para el desarrollo, se empleó una metodología cualitativa, con la que hizo la exploración exhaustiva de literatura relacionada con las tendencias y herramientas clave, posteriormente se realizó un análisis comparativo de estas herramientas en función de su eficacia, su adaptabilidad y la facilidad de implementación. Los resultados obtenidos, evidenciaron que la IA tiene el potencial de detectar y dar una rápida respuesta a las posibles amenazas, lo que permite optimizar la gestión de la seguridad informática por medio de procesos de automatización de tareas, a la vez que promueve una mayor cultura de seguridad entre estudiantes y empleados. Se concluyó que el apropiamiento de las tecnologías evaluadas ayuda a fortalecer la seguridad informática, a la vez que mejora la gestión de recursos, promoviendo un entorno educativo seguro y resiliente.

PALABRAS CLAVE: educación; ciberseguridad; inteligencia artificial; herramientas de seguridad; protección de datos; automatización de seguridad

1. Introducción

En el contexto actual, las instituciones educativas se enfrentan a desafíos cada vez mayores en términos de ciberseguridad. La creciente digitalización y el uso intensivo de tecnologías de la información han expuesto a estas organizaciones a una variedad de amenazas cibernéticas que pueden comprometer datos sensibles, interrumpir actividades académicas y dañar la reputación institucional. Una alternativa para hacer frente a estos desafíos es la integración de herramientas de ciberseguridad basadas en Inteligencia Artificial (IA).

La IA en ciberseguridad representa un avance significativo, permitiendo a las instituciones educativas no solo detectar y responder a amenazas en tiempo real, sino también anticiparse a posibles ataques mediante análisis predictivo y aprendizaje automático. Las herramientas que emplean IA en este ámbito están diseñadas para identificar comportamientos anómalos, analizar el tráfico de red y los comportamientos de los usuarios, y mitigar riesgos de manera proactiva. Estas soluciones avanzadas proporcionan una defensa adaptativa que se ajusta continuamente a nuevas amenazas, ofreciendo una protección robusta y efectiva contra una amplia gama de ciberataques.

En este sentido, las soluciones de ciberseguridad basadas en IA facilitan la visibilidad y el control total de la infraestructura de TI, permitiendo a las instituciones educativas gestionar la seguridad de manera centralizada y eficiente. Estas herramientas no solo mejoran la capacidad de respuesta a incidentes, sino que también contribuyen a la optimización de recursos, liberando a los equipos de seguridad de tareas manuales y permitiéndoles enfocarse en actividades estratégicas. La integración de estas tecnologías en el entorno educativo no solo garantiza la protección de datos sensibles y la continuidad de las actividades académicas, sino que también fomenta una cultura de seguridad y concienciación entre estudiantes y personal.

MÉTODOS

La metodología utilizada en este artículo se enmarca en un enfoque cualitativo, El proceso comenzó con un análisis exhaustivo de referentes bibliográficos, donde se revisó la literatura existente sobre herramientas de ciberseguridad que integran inteligencia artificial en el ámbito educativo. Esta revisión bibliográfica permitió identificar tendencias, enfoques y tecnologías clave. Posteriormente, se desarrolló un cuadro de comparación de las herramientas más relevantes, evaluando criterios como eficacia, adaptabilidad y facilidad de integración en las instituciones educativas. Esta comparación cualitativa se basó en la interpretación de las características y capacidades de cada herramienta, buscando ofrecer una visión integral y crítica de su aplicación en el contexto específico de la ciberseguridad educativa. Así, la metodología cualitativa empleada en este artículo permitió profundizar en el análisis de las tecnologías emergentes y su impacto en el entorno académico.

A partir del análisis de herramientas de inteligencia artificial para la detección de ciberamenazas en tiempo real en el sector educativo, se propone una metodología que facilite estudios comparativos similares y optimice la selección de soluciones. Esta metodología inicia con la definición del alcance y objetivos, donde se establecen los requisitos específicos de seguridad para el contexto educativo sobre los tipos de ciberamenazas que se desean mitigar. Luego, se realiza una selección de herramientas en función de sus características donde se destaca la capacidad de integración en entornos educativos. Posteriormente, se identifican criterios de evaluación que incluyen precisión en la detección, facilidad de uso, capacidad de respuesta en tiempo real y costo de implementación, permitiendo que los parámetros reflejen adecuadamente las necesidades del sector.

Con base en estos criterios, se lleva a cabo un análisis comparativo mediante cuadros visuales que destacan las fortalezas y limitaciones de cada herramienta, ofreciendo una visión clara de su efectividad en diferentes áreas. La metodología también incluye una evaluación del impacto educativo, examinando los posibles beneficios y desafíos que implica implementar estas soluciones en el ambiente de aprendizaje. Finalmente, se presentan conclusiones que sintetizan los hallazgos y orientan hacia la selección de herramientas de ciberseguridad que, además de cumplir con los requisitos técnicos, aporten un valor educativo, promoviendo un entorno de aprendizaje seguro y confiable.

La metodología de tipo cualitativa planteada en este artículo se dispone en etapas clave que permiten conseguir una selección óptima de herramientas de ciberseguridad con inteligencia artificial en el entorno educativo, a partir de la definición de objetivos específicos de seguridad, se proponen los criterios de selección que contemplan precisión, facilidad de uso y viabilidad económica, adecuados al contexto educativo. Con estos parámetros, se llevó a cabo un análisis comparativo detallado, que busca ilustrar las características de cada herramienta de forma que permitan resaltar sus respectivas capacidades de respuesta en la detección de amenazas en tiempo real, así como su integración en sistemas académicos. De igual forma, se evaluó el potencial impacto, considerando por un lado los beneficios y por otro lado los retos que cada tecnología puede aportar en el sector de la educación. En este sentido, los hallazgos se orientan hacia soluciones que no sólo aborden necesidades técnicas, sino que también refuercen la seguridad de manera efectiva y adaptativa.

2. Resultados

Teoría y Conceptualización

La inteligencia artificial (IA) y la seguridad informática están cada vez más interconectadas debido a la capacidad de automatizar numerosos procesos de ciberseguridad mediante técnicas como el aprendizaje automático. Históricamente, las acciones de seguridad informática dependían en gran medida de la experiencia humana, lo cual presentaba desventajas como el cansancio y la monotonía que afectan la eficiencia y precisión. Sin embargo, la IA ofrece una alternativa efectiva al permitir el desarrollo de algoritmos basados en datos de incidentes pasados. Estos algoritmos pueden prever futuros ataques con cierto margen de error, lo que ayuda a mitigar su impacto en las organizaciones (Castro, 2022).

¿Qué es la IA para la ciberseguridad?

La Inteligencia Artificial (IA) en el ámbito de la ciberseguridad se refiere al uso de tecnologías avanzadas para detectar, prevenir y responder a amenazas cibernéticas. Esta disciplina aplica algoritmos de aprendizaje automático, procesamiento del lenguaje natural y otras técnicas sofisticadas para analizar grandes volúmenes de datos, identificar patrones anómalos y predecir posibles amenazas. (Martín, 2024)

La IA permite una respuesta más rápida y efectiva mediante la automatización de la detección y la reacción frente a incidentes. Explica Nolasco-Mamani, et al, 2022 que los sistemas basados en IA aprenden continuamente de datos históricos y en tiempo real, lo que les permite identificar comportamientos sospechosos y actuar de manera proactiva. Esta capacidad de aprendizaje y adaptación es esencial en un entorno donde las amenazas son cada vez más sofisticadas y variadas.

Por otra parte, la IA utiliza algoritmos de aprendizaje automático para realizar análisis predictivos, permitiendo anticipar ciberataques antes de que ocurran. Al analizar patrones de datos y comportamientos previos, los sistemas de IA pueden identificar vulnerabilidades y prever posibles escenarios de ataque, brindando a las organizaciones una ventaja estratégica en la protección de sus activos digitales. (Toquiantzi, 2022)

A continuación, se describen algunos términos importantes de esta disciplina:

Aprendizaje automático (Machine Learning): es el aprendizaje de un ordenador sin ser necesariamente programado. Uno de los métodos de algoritmos de aprendizaje más estudiado es el llamado redes neuronales, que se basan en la imitación del cerebro, los avances en los estudios del funcionamiento del cerebro han dado resultados importantes y han acelerado los resultados de la IA García V, et al (2020).

Aprendizaje profundo: no solo se enfoca en la adquisición de conocimientos, también se aplica en la práctica de estos en situaciones reales. lo que conlleva una un cambio de cultura educativa, donde los integrantes estudiantes profesores adquieren nuevas formas de entender el aprendizaje. Las competencias globales de aprendizaje profundo también se conocen como las 6Cs, que integran carácter, ciudadanía, colaboración, comunicación, creatividad y pensamiento crítico. Estas competencias son importantes para que los estudiantes puedan prosperar en un mundo cada vez más competitivo. El aprendizaje profundo también motiva la participación de los estudiantes, formándose como agentes de cambio ante la sociedad Quinn, et al (2021).

Modelos Híbridos Combinación de diferentes técnicas de IA y aprendizaje automático

Los modelos híbridos en ciberseguridad integran múltiples técnicas de inteligencia artificial (IA) y aprendizaje automático (Machine Learning) para mejorar la detección de amenazas, creando sistemas más precisos y robustos ante ataques avanzados y cambiantes. Estos modelos combinan enfoques de detección basados en firmas tradicionales con técnicas de aprendizaje profundo y aprendizaje por refuerzo, lo que permite que el sistema aprenda patrones complejos y responda dinámicamente ante nuevas amenazas. Al integrar enfoques como redes neuronales profundas y modelos generativos, los sistemas híbridos son capaces de reconocer patrones de comportamiento malicioso y reducir significativamente las tasas de falsos positivos. Además, algunos de estos sistemas emplean explicabilidad (XAI) y gráficos de conocimiento, lo que facilita la interpretación de las decisiones de detección y optimiza el proceso de mitigación de amenazas. La combinación de técnicas permite un análisis profundo y adaptable, crucial para proteger infraestructuras críticas y redes empresariales en un entorno de amenazas creciente y cada vez más sofisticado Yaseen (2023).

Procesamiento del Lenguaje Natural (NLP)

El Procesamiento del Lenguaje Natural (NLP) es esencial en la detección de amenazas, especialmente en el análisis de correos electrónicos y mensajes sospechosos. Los algoritmos de NLP ayudan a identificar patrones lingüísticos comunes en ataques de phishing, estafas y otras amenazas cibernéticas. Estas herramientas permiten analizar el contexto, la sintaxis y el tono de los mensajes, facilitando la identificación de intentos de ingeniería social y otras tácticas de manipulación en tiempo real (Arazzi et al., 2023; Alhogail & Alsabih, 2021). Al combinar técnicas como el modelo TF-IDF y el análisis de sentimientos, el NLP permite detectar palabras clave y frases que suelen usarse en contenido malicioso, aumentando la precisión en la clasificación de amenazas y fortaleciendo las capacidades de ciberseguridad en entornos empresariales y personales (Yin et al., 2021). Esta capacidad de analizar texto a gran escala contribuye significativamente a la defensa proactiva en sistemas de seguridad de correo electrónico y redes sociales, donde las amenazas de phishing y ciberacoso son frecuentes (Basheer et al., 2021).

Tipos de sistemas y analítica con Integración de la IA

Según (García, V, et al. 2020) La sociedad del conocimiento exige cambios urgentes en los sistemas educativos del mundo. Estos cambios deben ir de la mano con las nuevas tecnologías y los servicios intangibles. En el contexto de la educación superior, la seguridad de la información se ha convertido en un componente crucial para proteger datos sensibles y garantizar un entorno digital seguro. La inteligencia artificial (IA) ha revolucionado este campo, proporcionando herramientas avanzadas para la detección y prevención de amenazas. A continuación, se presentan las principales tecnologías de seguridad basadas en IA: Leandro Baez 24072024

ISSN 2952-2560

Sistemas de Detección y Prevención de Intrusiones (IDPS) basados en IA: Estos sistemas utilizan algoritmos avanzados para identificar actividades maliciosas en tiempo real, protegiendo la infraestructura y sistemas de las instituciones educativas.

Análisis de Comportamiento del Usuario y Entidades (UEBA): Mediante el análisis del comportamiento de entidades, estas herramientas ayudan a detectar actividades sospechosas donde se generan posibles amenazas internas.

Seguridad Basada en Identidad (Identity Access Management – IAM): Estas soluciones garantizan que sólo los usuarios autorizados tengan acceso a los recursos sensibles, gestionando identidades y controlando accesos de manera segura.

Sistemas de Gestión de Información y Eventos de Seguridad (SIEM): Los sistemas SIEM recopilan, analizan y correlacionan datos de eventos de seguridad en tiempo real, proporcionando una visión integral de la seguridad de la infraestructura.

Protección de Datos y Prevención de Pérdida de Datos (DLP): Las soluciones DLP monitorizan y protegen los datos sensibles contra fugas y accesos no autorizados, garantizando la confidencialidad y la integridad de la información.

Automatización y Orquestación de Seguridad (SOAR): Estas herramientas automatizan la respuesta a incidentes de seguridad, coordinando las acciones necesarias para mitigar amenazas de manera eficiente y rápida.

Análisis de Amenazas y Caza de Amenazas (Threat Hunting): Utilizando técnicas avanzadas de análisis de búsqueda proactiva, estas herramientas identifican neutralizando amenazas que podrían haber pasado desapercibidas por otros sistemas.

La adopción de tecnologías de seguridad basadas en inteligencia artificial en la educación superior no solo mejora la protección de la información contra diversas amenazas cibernéticas, sino que también optimiza la gestión de la seguridad al automatizar tareas de respuestas a incidentes. Esto permite a las instituciones centrar más recursos en su principal misión educativa, mejorar su reputación y confianza, garantizar el cumplimiento normativo fomentando un entorno de innovación. (Anchala, 2024).

En el siguiente apartado, se exploran en detalle las características, servicios y beneficios de algunas de las herramientas más destacadas en este ámbito, destacando su impacto en las estrategias de ciberseguridad.

3. Discusión

Tabla 1: Comparativo de herramientas para la investigación y contención de amenazas

Herramienta	Características	Servicios	Valor Agregado	Libre o Costo	Impacto en la Educación

arktrace	Algunas de sus características clave incluyen: Detección y Respuesta en Tiempo Real: Utiliza algoritmos de IA para identificar y neutralizar amenazas cibernéticas rápidamente, minimizando el daño potencial. Modelos de IA Personalizables: La plataforma puede aprender el comportamiento normal de la red y alertar sobre desviaciones. Interfaz de Usuario Intuitiva: La plataforma proporciona vistas detalladas de incidentes y permite capturas de paquetes para análisis forenses.	**Darktrace PREVENT:** Proactivo en la identificación de amenazas y endurecimiento de defensas. **Darktrace DETECT:** Monitoriza y detecta amenazas en tiempo real. **Darktrace RESPOND**: Responde automáticamente a incidentes de seguridad. **Darktrace HEAL**: Ayuda en la recuperación y mitigación de incidentes.	**Reducción de Tiempo de Respuesta**: Minimiza el tiempo entre la detección y la mitigación de amenazas. **Cobertura Completa del Ecosistema:** Ofrece visibilidad y protección en toda la red, incluyendo dispositivos móviles y endpoints. **Personalización y Escalabilidad:** Se adapta a las necesidades específicas de cada organización y puede escalar según el crecimiento del negocio.	**Darktrace es una solución de pago.** Ofrece diferentes planes y niveles de servicio según las necesidades y tamaño de la organización, con una prueba gratuita disponible para evaluar sus capacidades.	En el ámbito educativo, Darktrace puede tener un impacto significativo al proporcionar: **Seguridad de Redes Educativas:** Protege las redes de universidades y colegios contra ataques cibernéticos. **Formación y Conciencia en Ciberseguridad:** Facilita la formación en ciberseguridad, permitiendo a los estudiantes y personal educativo estar mejor preparados contra amenazas. **Protección de Datos Sensibles:** Salvaguarda información sensible de estudiantes y empleados, cumpliendo con normativas de privacidad y seguridad. El aporte general a nivel educativo se enfoca en mantener la integridad y seguridad de los entornos digitales.

Cisco Secure X	Visibilidad Unificada: Panel centralizado con visibilidad en tiempo real de eventos y alertas de seguridad. Automación y Orquestación: Automatiza tareas y flujos de trabajo de seguridad. Respuesta Rápida a Incidentes: Herramientas para investigación y contención de amenazas en tiempo real. Análisis y Contexto de Amenazas: Utiliza inteligencia de amenazas para proporcionar contexto y priorización efectiva.	Gestión de Incidentes: Facilita la gestión de incidentes desde la detección hasta la resolución. Detección y Respuesta de Amenazas: Herramientas avanzadas para la detección y respuesta en tiempo real. Integración y Orquestación de Seguridad: Soporte para soluciones de seguridad diversas y orquestación de flujos de trabajo. Análisis y Reportes: Proporciona análisis detallados y reportes personalizados.	Reducción de la complejidad Operativa: Centraliza la gestión de seguridad, reduciendo la complejidad. Mejora en la Respuesta a Amenazas: Automatizar flujos de trabajo y permite una respuesta más rápida. Mayor Visibilidad y Control: Ofrece una visión integral en tiempo real de la postura de seguridad.	No es gratuito; está disponible como parte de los paquetes de seguridad de Cisco.	Protección de Datos Sensibles: Ayuda a proteger datos sensibles de estudiantes y empleados. Cumplimiento Normativo: Facilita el cumplimiento de normativas específicas del sector educativo, como FERPA. Resiliencia Ante Amenazas: Mejora la capacidad de respuesta a incidentes, asegurando la continuidad educativa. Formación y Capacitación: Permite implementar programas de formación en ciberseguridad. Colaboración y Compartición de Información: Fomenta la colaboración y el intercambio de información sobre amenazas.

Vectra AI	Detección Automática de Amenazas: Utiliza algoritmos de aprendizaje automático para identificar comportamientos anómalos y patrones de ataque dentro de una red. Respuesta en Tiempo Real: Ofrece respuestas automáticas para mitigar riesgos, incluyendo el aislamiento de dispositivos comprometidos y la contención de actividades maliciosas. Análisis Profundo y Visibilidad Completa: Proporciona una visibilidad completa de las actividades en la red, con análisis detallados de eventos de seguridad. Priorización de Amenazas: Clasifica y prioriza las amenazas basándose en el nivel de riesgo y el impacto potencial. Integración con otras Soluciones de Seguridad: Se integra fácilmente con herramientas como SIEM (Security Information and Event Management) y SOAR (Security Orchestration, Automation, and Response).	Monitoreo Continuo: Vigilancia constante de redes y sistemas para detectar y responder a amenazas en tiempo real. Análisis Forense: Investigación post-incidente para comprender cómo ocurrió un ataque y cómo prevenir futuros incidentes. Soporte y Consultoría: Asistencia técnica y asesoramiento estratégico para la implementación y optimización de la herramienta. Informes y Alertas: Generación de informes detallados y alertas en tiempo real sobre incidentes de seguridad.	Eficiencia Mejorada: Automatiza tareas de detección y respuesta, reduciendo la carga de trabajo manual para los equipos de seguridad. Detección Temprana: Identifica amenazas en etapas tempranas, ayudando a prevenir daños significativos. Adaptabilidad: Los algoritmos de IA se actualizan continuamente para adaptarse a nuevas tácticas y técnicas de los atacantes. Optimización de Recursos: Permite una gestión más eficiente de los recursos de seguridad, enfocando esfuerzos en incidentes críticos.	Vectra AI es una herramienta comercial, por lo que su uso implica un costo.	Protección de Datos Sensibles: Vectra AI ayuda a proteger información confidencial, como datos personales de estudiantes y empleados, registros académicos, y propiedad intelectual. Seguridad en Redes Educativas: Monitorea las redes de las instituciones educativas para identificar y mitigar amenazas, garantizando un entorno seguro para el aprendizaje y la investigación. Prevención de Ataques Dirigidos: Identifica y responde a ataques dirigidos que buscan comprometer datos valiosos, minimizando el riesgo y el impacto de dichos ataques. Formación y Concienciación: Los datos y análisis proporcionados por Vectra AI pueden utilizarse para educar a estudiantes y empleados sobre ciberseguridad, mejorando la conciencia y preparación general en este campo. Optimización de Recursos: Automatiza tareas de seguridad, permitiendo que

					el personal de TI se concentre en actividades estratégicas y educativas, mejorando la eficiencia operativa.

crowdstrike	CrowdStrike nos ofrece una solución muy completa y robusta, además de actualizarse con gran frecuencia para que pueda ser capaz de detectar nuevas técnicas de atacantes El despliegue es sencillo, lo que no solo agiliza el proceso de protección, sino que además reduce los costos operativos. Al no basarse en firmas, la detección de amenazas y la posibilidad de respuesta a incidentes y colaboración para la caza de amenazas se simplifica notablemente. El cliente móvil de la solución da acceso a las potentes características de análisis de todo el endpoint, habilitando una rápida respuesta a la detección de amenazas, utilizado por su personal de seguridad y no solamente por su equipo de respuesta a incidentes.	Servicios de Respuesta a Incidentes CrowdStrike cuenta con un equipo de expertos en seguridad que se especializa en la respuesta a incidentes. Análisis Forense y de Amenazas La compañía ofrece análisis forense detallado y servicios de inteligencia sobre amenazas. Esto ayuda a las organizaciones a comprender mejor las tácticas, técnicas y procedimientos utilizados por los atacantes, lo que permite mejorar la preparación y respuesta ante futuros incidentes. Protección de Endpoints A través de su plataforma CrowdStrike Falcón, la empresa proporciona protección avanzada para endpoints. Esto incluye detección y respuesta en tiempo real, así como la capacidad de gestionar vulnerabilidades y proteger datos críticos.	CrowdStrike tiene diferencias clave con respecto a los antivirus tradicionales con los que se puede comparar en el mercado, como por ejemplo, McAfee. Basándonos inicialmente en la arquitectura, mientras que los antivirus tradicionales operan de forma local en una arquitectura on premise, Falcon utiliza una arquitectura específica para el endpoint, lo que permite ofrecer protección en cualquier lugar; ya sea a nivel de red/nube o a nivel on premise. Identifica y detiene las amenazas con el objetivo de reducir su exposición al riesgo. Aborda multitud de formas de malware y de ataques, incluyendo exploits, scripts maliciosos, ransomware y mucho más	Herramienta con costo; sin embargo;ofrece dos planes distintos según necesidades	Detección y prevención de ciberataques CrowdStrike utiliza inteligencia artificial para detectar y prevenir posibles ciberataques, evitando daños críticos a las empresas con las que trabaja. Su herramienta CrowdStrike Falcon Cloud Security está diseñada específicamente para "detener las infracciones en la nube". La plataforma CrowdStrike Falcon ofrece visibilidad, detección y protección en tiempo real contra todo tipo de ataques basados en identidad. CrowdStrike fue nombrada líder en el IDC MarketScape: Worldwide Risk-Based Vulnerability Management Platforms 2023 Vendor Assessment. Esto demuestra su capacidad para ayudar a las empresas a gestionar eficazmente sus vulnerabilidades de seguridad.

Fuente: Elaboración propia 2024

Herramientas de IA para ciberseguridad que necesitas implementar en tu empresa este 2024

- Darktrace

Darktrace es una empresa de ciberseguridad que emplea inteligencia artificial (IA) para ofrecer una protección avanzada contra amenazas cibernéticas. Su tecnología, conocida como Cyber AI Loop, utiliza múltiples modelos de IA para monitorear, detectar y responder continuamente a posibles amenazas en tiempo real. Entre sus características clave se encuentra la IA autoaprendizaje, que se adapta constantemente para entender el comportamiento normal de la red de una organización, facilitando la detección de anomalías. Darktrace PREVENT se enfoca en identificar y abordar de manera proactiva las posibles debilidades de seguridad, mientras que Darktrace DETECT and RESPOND proporciona detección de amenazas en tiempo real para generar capacidades de respuesta autónoma, permitiendo mitigar rápidamente amenazas sin interrumpir las operaciones normales.

La plataforma ActiveAI Security de Darktrace ofrece un enfoque proactivo de ciberseguridad, proporcionando visibilidad completa de las rutas de ataque, investigación automatizada de amenazas proporcionando mecanismos de defensa preventivos. También han desarrollado modelos para abordar los riesgos asociados con el uso de herramientas de IA generativa, ayudando a prevenir la fuga de datos, de esta manera proteger la propiedad intelectual. Sus soluciones incluyen inteligencia de amenazas con respuesta a incidentes con soporte 24/7 por un equipo de analistas cibernéticos, así como la automatización de la investigación sobre las respuestas a alertas, lo que reduce la carga de trabajo en los equipos de seguridad mejorando la eficiencia.

El enfoque de Darktrace, impulsado por IA, asegura que las organizaciones de educación superior puedan mantenerse a la vanguardia de las amenazas cibernéticas sofisticadas. Proporciona soluciones de seguridad dinámicas, adaptativas e inteligentes que ayudan a gestionar el riesgo cibernético, cumplir con los requisitos regulatorios para la protección de datos sensibles en un entorno educativo en constante evolución.

- Vectra AI

Vectra AI se destaca como una herramienta avanzada que integra la Inteligencia Artificial para detectar y responder a amenazas complejas en tiempo real, explica IBRAHIM, 2022. Esta plataforma se especializa en identificar comportamientos anómalos y patrones de ataque dentro de una red, proporcionando a los equipos de seguridad información valiosa y accionable para actuar rápidamente ante incidentes.

La herramienta utiliza algoritmos de aprendizaje automático para analizar el tráfico de red y los comportamientos de los usuarios, lo que le permite detectar amenazas que podrían pasar desapercibidas para las soluciones de seguridad tradicionales. Esta capacidad es fundamental para identificar ataques dirigidos y movimientos laterales dentro de la red, aspectos críticos en la protección de cualquier entorno digital. (IBRAHIM, 2022)

La plataforma no solo detecta amenazas, sino que también ofrece respuestas automáticas para mitigar riesgos de manera inmediata. Esto incluye el aislamiento de dispositivos comprometidos y la contención de actividades maliciosas, evitando así la propagación del ataque y minimizando su impacto.

Aplicabilidad de Vectra AI en Procesos Educativos

Vectra AI no solo es aplicable en entornos corporativos y empresariales, sino que también puede ser una herramienta valiosa en las instituciones de educación superior. Estas manejan una gran cantidad de datos sensibles, incluyendo información personal de estudiantes y empleados, registros académicos, y propiedad intelectual. La protección de estos datos es crucial para mantener la confianza y cumplir con las regulaciones de privacidad y seguridad.

Protección de Datos Sensibles: Las instituciones educativas manejan información confidencial que necesita ser protegida contra accesos no autorizados y filtraciones. Vectra AI puede ayudar a detectar y mitigar amenazas que intenten comprometer esta información, asegurando que los datos personales y académicos estén protegidos. (Vikhyath, 2022)

Seguridad en Redes Educativas: Las redes de las instituciones de educación superior suelen ser extensas y variadas, conectando múltiples dispositivos y usuarios. Vectra AI puede monitorear estas redes en tiempo real, identificando comportamientos anómalos y amenazas potenciales, y proporcionando una respuesta rápida para prevenir incidentes de seguridad.

Prevención de Ataques Dirigidos: Las instituciones educativas pueden ser objetivos de ataques dirigidos debido a la valiosa información que poseen. Con base en Nurmi, 2021, Vectra AI puede identificar estos ataques en etapas tempranas, permitiendo una respuesta oportuna y minimizando el daño potencial.

Formación y Concienciación: Al integrar Vectra AI, las instituciones educativas pueden utilizar los datos y análisis proporcionados por la herramienta para educar a estudiantes y empleados sobre las mejores prácticas en ciberseguridad. Esto puede incluir la identificación de amenazas comunes y cómo responder a ellas, mejorando la conciencia y preparación general en seguridad cibernética.

De igual forma, Vectra AI se destaca por ofrecer un enfoque orientado hacia la visualización de amenazas por medio de interfaces intuitivas, facilitando la comprensión del estado de la seguridad de los sistemas en tiempo real, situación particularmente útil en entornos empresariales con recursos limitados. En comparación con otras soluciones, Vectra AI emplea una perspectiva adaptativa que aprende de entornos específicos, actualizando y modificando su funcionamiento a partir de la detección de nuevos patrones de comportamiento, esto permite mejorar la precisión en la identificación de amenazas emergentes y desconocidas. Así mismo, faculta la fácil integración con otras plataformas de seguridad, contribuyendo a una respuesta más coordinada y eficaz frente a incidentes complejos.

Finalmente, es de notar que existe otra característica importante es su capacidad para la priorización de amenazas en función del riesgo, con la que puede optimizar la respuesta al permitir que los equipos de seguridad se enfoquen en los ataques más críticos, a la vez que gestiona los recursos de manera más eficiente, para el contesto educativo esto resulta particularmente relevante, ya que los departamentos de tecnología podrían enfrentarse a restricciones de personal o presupuesto, finalmente, Vectra AI promueve un punto de vista proactivo para la gestión de la ciberseguridad, ofreciendo recomendaciones y análisis predictivos que ayudan a las instituciones a anticipar posibles vulnerabilidades antes de que se conviertan en incidentes.

- Cisco Secure X

De acuerdo Cisco (2021) Cisco SecureX es una plataforma de seguridad integrada y nativa en la nube que conecta la cartera de seguridad de Cisco con la infraestructura del usuario. En el sector educativo, SecureX proporciona visibilidad unificada, automatización y eficiencia operativa, protegiendo redes, endpoints, nubes y aplicaciones. Facilita la detección y respuesta rápida a amenazas, permitiendo a las instituciones educativas mantener un entorno seguro y centrarse en su misión principal de enseñanza y aprendizaje

Automatización y Orquestación: SecureX permite automatizar tareas repetitivas y críticas de seguridad, como la investigación de amenazas y la respuesta a incidentes, lo que reduce el tiempo y los costos operativos. Esto es crucial en el sector educativo, donde los recursos pueden ser limitados.

Integración y Visibilidad: SecureX integra múltiples tecnologías de detección y sensores en una única plataforma, proporcionando una visibilidad unificada y capacidades de orquestación. Esto ayuda a las instituciones educativas a gestionar y proteger su infraestructura de red, usuarios y dispositivos de manera más eficiente.

Respuesta a Incidentes: La plataforma permite una respuesta rápida y coordinada a incidentes de seguridad, reduciendo el tiempo de permanencia de las amenazas y minimizando el daño potencial. Esto es vital para proteger la información sensible de estudiantes y personal en entornos educativos.

Adaptabilidad y Escalabilidad: SecureX está diseñado para adaptarse a diferentes infraestructuras tecnológicas y escalar conforme a las necesidades cambiantes de las instituciones educativas. Esto permite a las escuelas y universidades ajustarse fácilmente a cambios en el volumen de tráfico o a la incorporación de nuevos dispositivos y usuarios, manteniendo un nivel de seguridad adecuado sin comprometer el rendimiento.

Capacidades Analíticas Avanzadas: La plataforma ofrece herramientas de análisis de seguridad que permiten a las instituciones educativas identificar patrones y tendencias en amenazas potenciales. Con estas capacidades, es posible predecir posibles vulnerabilidades, lo que mejora la prevención de ataques.

Interfaz Intuitiva y Personalizable: SecureX cuenta con una interfaz intuitiva que permite a los administradores personalizar su configuración y panel de control. Esta flexibilidad facilita la administración de seguridad, permitiendo una gestión más efectiva incluso a usuarios con recursos técnicos limitados.

Fortalecimiento de la Colaboración en Equipos de Seguridad: SecureX permite una colaboración más fluida entre equipos de seguridad al integrar flujos de trabajo y herramientas, lo cual es esencial en un entorno educativo donde los recursos pueden ser compartidos entre diferentes campus o unidades Cisco (2021).

- Crowdstrike

La misión de Crowdstrike es recoger y analizar toda la telemetría desde cada endpoint que se intercomunica con su servicio y así detectar, de manera proactiva y predecir amenazas avanzadas en el ambiente a partir de sistemas protegidos en el perímetro. La suite en la nube de Crowdstrike es la Web Console.

CrowdStrike utiliza técnicas de detección de amenazas y análisis de comportamiento en el endpoint del usuario. Extrae el funcionamiento de todas las aplicaciones con una caracterización denominada Indicator of Attack (IOA) y un sofisticado Byte Level de detección de amenazas. Lo llamativo es que, al ser una solución en la nube, cualquier regla o modificación dentro de la plataforma impacta en todos los clientes, formando una comunidad de usuarios no solo en base de conocimiento de amenazas sino también una comunidad auto protegida. Su efectiva solución está en la delgadez del agente o sensor, la aplicación transparente y la correcta explotación de todos estos sensores. No se necesita implementar servidores de visibilidad dentro de las instalaciones del usuario a diferencia de la mayoría de las soluciones existentes (de la competencia), ya que la solución funciona como servicio en la nube en modo SAAS.

El endpoint (custodiado por CrowdStrike o cualquier otra solución de protección como Symantec) se convierte en un generador de sensores o IOAs y realiza peticiones por algoritmo para identificar las amenazas de que se trate a través del CrowdStrike Threat Graph. En el caso de ataques en curso, ya sea que los sensores estén o no activos en la Read

CrowdStrike Engagement es una plataforma de gestión de equipos de seguridad con capacidades avanzadas como el acceso a la inteligencia de amenazas de CrowdStrike

Intelligence, el envío de alertas a través de APIs o integraciones con otras plataformas de seguridad y servicios de notificación, y la capacidad para reconocer cadenas de comandos e identificar a los usuarios ofensivos mediante las capacidades del MITRE ATT&CK Framework. Entre los principales componentes de la plataforma de management de soluciones cloud de CrowdStrike, encontramos un dashboard con un panel que muestra el número de hosts reportados por hora y se puede seleccionar el vídeo con el recorrido que ha seguido el host para llegar a esa alerta.

Por otra parte como lo menciona (Arango, 2022) la solución de prevención gestionada de amenazas CrowdStrike Falcon Protección proporciona una protección avanzada (EPP - Endpoint Protection Platform) contra las explotaciones, los fallos de seguridad de día cero, malware, ransomware y Memory, además de que ha sido acreditado por los analistas externos de pruebas colectivas de AV-Comparatives durante la mayoría de los años, cumpliendo las pruebas de cumplimiento mensual anunciadas en las pruebas Mac, así como el Mensual de Malware Scene y Test. Falco on-premises es una solución de prevención de tecnologías destinada a las amenazas Linux, incluye un motor de reglas de código abierto que viene con un conjunto de reglas de detección comunes para el compromiso del contenedor y complementa la cobertura de prevención del host en ambientes que utilizan el sistema operativo Linux.

Comparativa con antivirus:

El producto CrowdStrike ya no debe ser comparado con antivirus. CrowdStrike puede ser considerado como un producto sustituto de un antivirus. Los antivirus de hace 20 años no han evolucionado y actualmente se encuentran disponibles antivirus con motores mucho más avanzados. Sin embargo, el motor de detección de CrowdStrike se encuentra mucho más avanzado frente a los motores de detección de antivirus corrientes. Actualmente utilizo la marca (Sophos de próxima generación) con una capacidad de detección que se extiende a varias capas como Sophos Clean, EDR e IPS (no sólo un motor de firma) me sea económicamente viable y si a un socio autorizado de CrowdStrike le es posible entablar una negociación con Sophos se consideraría algún cambio. CrowdStrike llega tarde a la batalla, pero llega para instaurar un nuevo concepto en la protección de endpoints.

Comparativa con firewalls para protección perimetrales y/o internas:

He cambiado la consideración de inicio realizada, CrowdStrike no es una herramienta que reemplaza a un firewall de próxima generación, respuesta menos avanzada, no contamos con otro administrador interno en la organización y la capacidad de nuestro proveedor de servicio Managed Security Service Provider (MSSP) no conviene redundar. CrowdStrike es una herramienta supervisora, analítica y algorítmica, su función principal es detección temprana. Entonces será una solución eficaz en su área de expertise reduciendo su capacidad de respuesta. CrowdStrike se explica principalmente con su fase de maquinaria administrativa response y no en su fase de control de políticas y aprovisionamiento.

ISSN 2952-2560

CONCLUSIONES

El análisis de herramientas de ciberseguridad con integración de IA para el sector o instituciones de educación superior demuestra que la adopción de tecnologías avanzadas, como el aprendizaje automático y el procesamiento de datos en tiempo real, es esencial para proteger la infraestructura educativa frente a amenazas cibernéticas cada vez más complejas. Estas herramientas mejoran la detección y respuesta ante incidentes, al tiempo que permiten la identificación proactiva de vulnerabilidades, manteniendo a las universidades un paso adelante frente a los atacantes.

La detección de ciberamenazas en tiempo real en el sector educativo evidencia una necesidad urgente de implementar soluciones tecnológicas que fortalezcan la seguridad y protección de datos en entornos académicos. La revisión comparativa de estas herramientas permite identificar fortalezas, limitaciones y enfoques específicos de cada solución, facilitando la selección de tecnologías adecuadas para el ámbito educativo. Los cuadros comparativos presentados en el artículo destacan tanto los servicios de seguridad que ofrecen como su impacto potencial en el proceso educativo, donde proteger la información resulta esencial para asegurar la continuidad operativa y preservar la privacidad de la comunidad educativa.

Las plataformas de seguridad integradas y nativas en la nube aportan múltiples beneficios a las instituciones educativas, donde la protección de datos y la eficiencia operativa son esenciales. Este tipo de solución permite una visibilidad centralizada y capacidades de orquestación, lo que facilita la automatización de tareas repetitivas de seguridad, optimizando los tiempos de respuesta ante incidentes y mejorando la eficiencia en contextos donde los recursos suelen ser limitados. Además, la adaptabilidad y escalabilidad de estas plataformas aseguran que puedan ajustarse al volumen de tráfico y al número de dispositivos o usuarios en crecimiento, sin comprometer el rendimiento o la seguridad. Las herramientas de análisis permiten identificar patrones de riesgo y prever vulnerabilidades, mejorando la capacidad de prevención. Con una interfaz personalizable e intuitiva, estas plataformas facilitan la gestión de la seguridad, promoviendo la colaboración entre los equipos y permitiendo la integración de herramientas compartidas. Estas cualidades son fundamentales para proteger tanto la infraestructura tecnológica como la información de estudiantes y personal, ayudando a las instituciones a concentrarse en su misión educativa sin comprometer la seguridad.

Este análisis también aporta una visión clara sobre cómo las herramientas de inteligencia artificial pueden fomentar una cultura de ciberseguridad en instituciones educativas, creando un entorno propicio para el aprendizaje y la innovación. La incorporación de estas tecnologías en la educación no solo responde a amenazas actuales, sino que también prepara a los estudiantes para un futuro en el que la ciberseguridad será un componente crucial en cualquier campo profesional. La automatización impulsada por IA optimiza la eficiencia de los equipos de seguridad, fortaleciendo la resiliencia institucional generando un entorno digital seguro, ideal para el aprendizaje y la innovación.

La implementación de Vectra AI en el sector educativo ofrece un enfoque revolucionario para la lucha contra las ciberamenazas en tiempo real, particularmente al considerar la creciente complejidad y frecuencia de los ataques en entornos que manejan información sensible y deben garantizar la seguridad y privacidad de los datos. Por medio de los algoritmos de aprendizaje automático y monitoreo constante, Vectra AI se ha venido posicionando como una solución robusta capaz de detectar patrones anómalos y realizar intervenciones automáticas, característica esencial al momento de proteger los sistemas informáticos educativos actuales cada vez más complejos y multidimensionales. De esta manera, Vectra AI ayuda a proteger datos confidenciales, a la vez que fortalece la resiliencia de las instituciones académicas al proponer alternativas para el análisis forense detallado y la priorización de las amenazas cibernéticas, ayudando en la optimización de los recursos, permitiendo además que los equipos de seguridad educativa se enfoquen en tareas estratégicas. Al incorporar una herramienta como esta, las instituciones educativas pueden no solo cumplir con regulaciones de seguridad y privacidad, sino también fomentar una cultura de concienciación en ciberseguridad entre estudiantes y personal, aumentando la preparación colectiva ante posibles amenazas.

Referencias

Alhogail, A., & Alsabih, M. (2021). *Using NLP for cyber threat detection and analysis in social engineering attacks*. Journal of Cybersecurity and Privacy, 3(2), 99-114. https://doi.org/10.3390/jcp3020006

Anchala Sanez, Mauricio Rodolfo (2024) Propuesta de gestión de incidentes de seguridad, mediante la integración de inteligencia de amenazas para la contención de ataques informáticos. Maestría en Seguridad Informática, Quito: Universidad Israel 2024, 50p. Mg. Toasa Guachi Renato Mauricio Ph.D. Urdaneta Herrera Maryory, UISRAEL-EC-MASTER-SEG-INF-ART- 378.242-2024-002 http://repositorio.uisrael.edu.ec/handle/47000/4184

Arazzi, E., Gao, J., & Xu, S. (2023). *Recent advancements in machine learning for cybercrime prediction*. arXiv preprint arXiv:2304.04819. https://arxiv.org/abs/2304.04819

Arango, O. D. (2022). Detección de amenazas informáticas de tipo Malware Bancario o Ransomware Móvil hacia dispositivos Android, integrando IOC en una técnica semiautomatizada y con base en comportamientos analizados de incidentes.. Recuperado de: http://hdl.handle.net/20.500.12622/5700.

Arfeen, Muhammad & Ahmed, Saad & Khan, Muhammad & Jafri, Syed. (2021). E*ndpoint Detection & Response: A Malware Identification Solution*. 1-8. 10.1109/ICCWS53234.2021.9703010

Basheer, R., Ali, F., & Jones, R. (2021). *AI and NLP for phishing email detection: Approaches and challenges*. Computers & Security, 103, 102155. https://doi.org/10.1016/j.cose.2021.102155

Castro Maldonado, John. (2022). Análisis de riesgos y vulnerabilidades de seguridad informática aplicando técnicas de inteligencia artificial orientado a instituciones de educación superior. 1. 151. https://www.researchgate.net/publication/359379099_analisis_de_riesgos_y_vulnerabilidades_de_seguridad_informatica_aplicando_tecnicas_de_inteligencia_artificial_orientadoa_instituciones_de_educacion_superior

Cisco. (2021). *Cisco SecureX: Data Sheet. Cisco Systems*, Inc. https://www.cisco.com/c/en/us/products/collateral/security/securex/secure-x-datasheet.pdf

CrowdStrike - *Nexsys Colombia*. (n.d.). Nexsys Colombia. https://www.nexsysla.com/co/fabricantes-nexsys/crowdstrike/

García V, et al (2020). *La inteligencia artificial en la educación*. https://dialnet.unirioja.es/servlet/articulo?codigo=8231632

G Karantzas, C Patsakis - Journal of Cybersecurity and Privacy, 2021 - mdpi.com. An empirical assessment of endpoint detection and response systems against advanced persistent threats

Ibrahim, A. (2022). *Breaking Barriers: How AI and ML are Redefining Cybersecurity Defense.* https://www.researchgate.net/profile/Ibra-Him-5/publication/380152244_Breaking_Barriers_How_AI_and_ML_are_Redefining_Cybersecurity_Defense_AUTHORSIBRAHIM_A/links/662d7d3108aa54017ac8933c/Breaking-Barriers-How-AI-and-ML-are-Redefining-Cybersecurity-Defense-AUTHORSIBRAHIM-A.pdf

Ibrahim, A. (2022). *Guardians of the Virtual Gates: Unleashing AI for Next-Gen Threat Detection in Cybersecurity*. https://www.researchgate.net/profile/Ibra-Him-5/publication/380152167_Guardians_of_the_Virtual_Gates_Unleashing_AI_for_Next-Gen_Threat_Detection_in_Cybersecurity/links/662d7f257091b94e93e01a9f/Guardians-of-the-Virtual-Gates-Unleashing-AI-for-Next-Gen-Threat-Detection-in-Cybersecurity.pdf

Martín Martín, M. L. (2024). *Inteligencia Artificial: Un estudio de su impacto en Ciberseguridad*. https://openaccess.uoc.edu/handle/10609/150519

Nolasco-Mamani, M. A., Vidaurre, S. M. E., & Choque-Salcedo, R. E. (2022). *Innovación y Transformación Digital en la Empresa. ACVENISPROH Académico*. https://acvenisproh.com/libros/index.php/Libros_categoria_Academico/article/view/49

Nurmi, T. (2021). *Network detection and reaction: case study: proof of concept for Vectra implementation*. https://www.theseus.fi/handle/10024/511234

Quinn, J., Mceachen, J., Fullan, M., Gardner, M., & Grummy, M. (2021). *Sumergirse en el aprendizaje profundo herramientas atractivas.* Safekat. https://edmorata.es/wp-content/uploads/2021/04/FULLAN.-Sumergirse-en-el-Aprendizaje-Profundo_prw.pdf

Toquiantzi, S. J. (2022). *Facultad de ingeniería* (Doctoral dissertation, Benemérita Universidad de Puebla). https://repositorioinstitucional.buap.mx/server/api/core/bitstreams/e8369c4e-25d9-4d83-9f5c-966c45e890de/content

Vikhyath, K. B., Kubsad, S. S., & Sunidhi, A. G. (2022, December). *Survey on Data Security with Intersection of AI and Blockchain*. In 2022 Fourth International Conference on Cognitive Computing and Information Processing (CCIP) (pp. 1-7). IEEE. https://ieeexplore.ieee.org/abstract/document/10058639

Yaseen, A. (2023). AI-DRIVEN THREAT DETECTION AND RESPONSE: A PARADIGM SHIFT IN CYBERSECURITY. International Journal of Information and Cybersecurity, 7(12), 25–43. Retrieved from https://publications.dlpress.org/index.php/ijic/article/view/73

Yin, C., Han, J., & Wu, S. (2021). *Sentiment analysis and NLP applications in cybersecurity*. IEEE Access, 9, 108550-108565. https://doi.org/10.1109/ACCESS.2021.3092902