Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Tendencias de Aprendizaje Automático Aplicadas en Ciberseguridad

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

Boletín de Ciberseguridad

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CSIRT Académico UNAD

E-boletín Informativo CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Veintiséis
Agosto de 2024

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CSIRT Académico UNAD

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Líder
CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernandez

Revisó
Ing. Daniel Felipe Palomo Luna
Docente Esp. Seguridad Informática

Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Tabla de Contenido

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín de Ciberseguridad

Boletín informativo Número 26

Agosto 2024

Tendencias de Aprendizaje Automático Aplicadas en Ciberseguridad

Autores:

Hernando José Peña Hidalgo
CSIRT Académico UNAD
https://orcid.org/0000-0002-3477-2645

Luis Fernando Zambrano Hernández
CSIRT Académico UNAD
https://orcid.org/0000-0002-4690-3526

Sonia Ximena Moreno Molano
Líder Maestría en Ciberseguridad
https://orcid.org/0009-0002-6133-5157

Néstor Raúl Cárdenas Corral
CSIRT Académico UNAD
https://orcid.org/0000-0003-3691-0148

Introducción

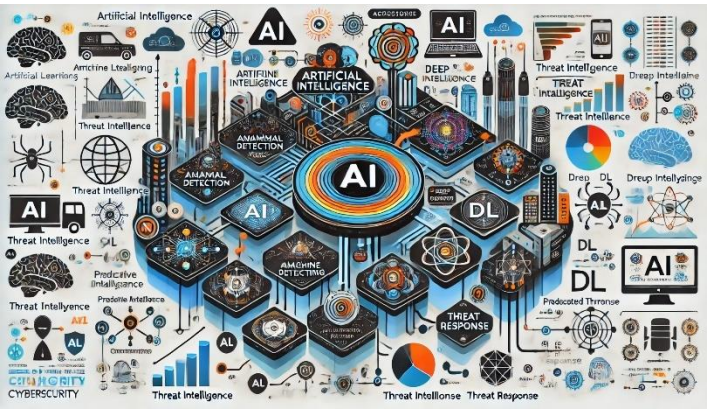


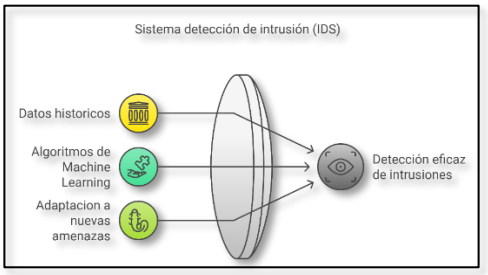
Ilustración 1. ChatGPT. (2024). Gráfica del ecosistema de inteligencia artificial y su contribución a la ciberseguridad. Gráfica generada por IA

El aprendizaje automático, como subconjunto de la inteligencia artificial, ha ganado una importante fuerza en el ámbito de la ciberseguridad debido a su capacidad para analizar grandes cantidades de datos e identificar patrones que pueden indicar actividades maliciosas. A medida que las amenazas cibernéticas se vuelven cada vez más sofisticadas, las medidas de seguridad tradicionales suelen resultar insuficientes, por lo que es necesario adoptar tecnologías avanzadas como el aprendizaje automático para reforzar las defensas (Martín, 2023).

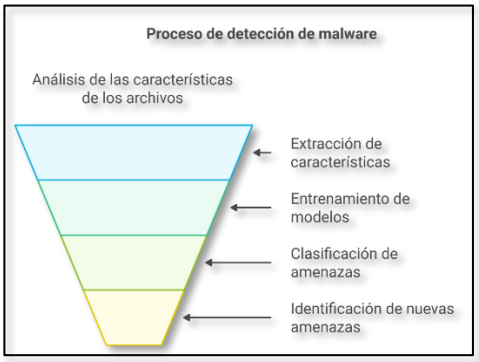
Desarrollo

Aplicación de Aprendizaje Automático en Ciberseguridad

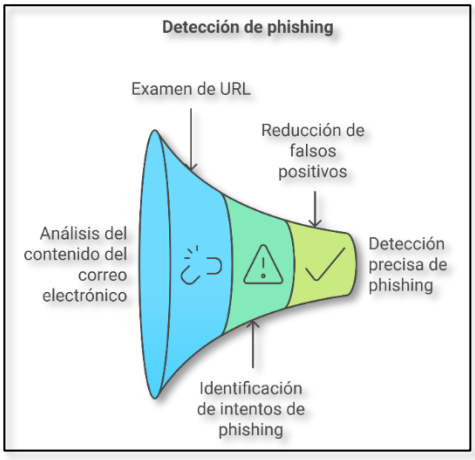
El avance del Aprendizaje Automático (AA) ha transformado significativamente el campo de la ciberseguridad, permitiendo el desarrollo de soluciones más robustas y adaptativas frente a las crecientes amenazas digitales.



Detección de intrusión: La detección de intrusión es una de las aplicaciones más efectivas del aprendizaje automático (AA) en ciberseguridad. Los algoritmos de AA se emplean para analizar continuamente el tráfico de la red, buscando patrones de comportamiento que puedan indicar actividades sospechosas o maliciosas. A diferencia de los sistemas tradicionales basados en firmas, que solo detectan amenazas conocidas, los modelos de AA tienen la capacidad de aprender de datos históricos, identificando patrones y tendencias en el tráfico legítimo, lo que les permite detectar anomalías en tiempo real(Sarker, 2021).



Detección de malware: La detección de malware es uno de los campos donde el aprendizaje automático (AA) ha demostrado ser especialmente eficaz, superando los métodos tradicionales basados en firmas o heurísticas. Los modelos de AA clasifican y detectan malware analizando una combinación de características estáticas y dinámicas de los archivos, lo que permite identificar tanto amenazas conocidas como variantes nuevas y en evolución. El uso de modelos de AA también ha permitido a los sistemas de detección de malware evolucionar hacia soluciones más rápidas y eficientes, como los motores de análisis en la nube que procesan grandes volúmenes de datos en tiempo real, ofreciendo protección inmediata contra nuevas amenazas (Kaspersky, 2020).



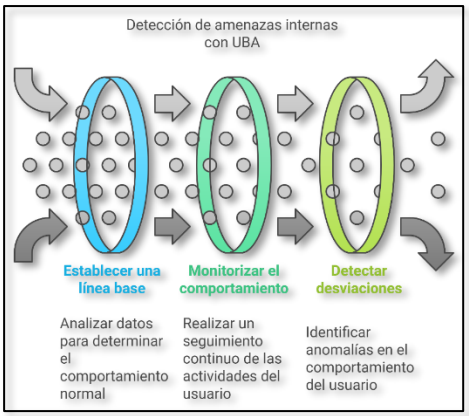
Detección de Phishing: El phishing sigue siendo una de las tácticas más utilizadas por los ciberdelincuentes para obtener información confidencial, como credenciales de acceso y datos personales. Para combatir esta amenaza, el aprendizaje automático (AA) ha emergido como una herramienta clave, utilizando técnicas avanzadas para analizar tanto el contenido del correo electrónico como las URL asociadas con posibles intentos de phishing.

Los modelos de AA aplicados a la detección de phishing emplean una variedad de enfoques. Primero, analizan el contenido del correo electrónico, buscando patrones sospechosos como el uso de lenguaje engañoso, errores ortográficos, urgencia exagerada y otros indicadores comunes de phishing

Boletín de Ciberseguridad

Análisis de Comportamiento mediante Aprendizaje Automático

El análisis de comportamiento es una técnica avanzada en ciberseguridad, especialmente cuando se utiliza aprendizaje automático (AA) para establecer líneas de base del comportamiento normal de los usuarios. Al observar y aprender de las actividades cotidianas, como los patrones de acceso, las aplicaciones utilizadas y los horarios de trabajo, el AA puede definir un perfil de comportamiento típico para cada usuario o dispositivo en la red.



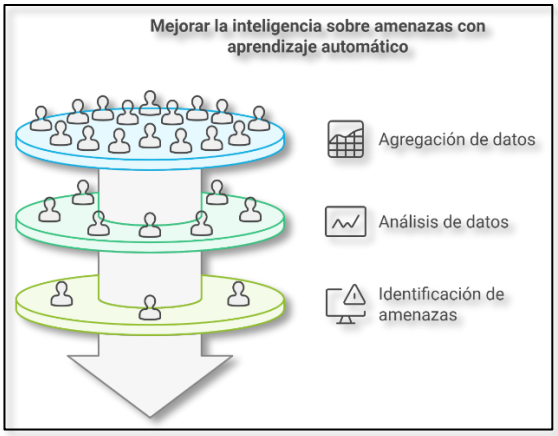
Una vez establecida esta línea de base, los algoritmos de AA pueden identificar desviaciones significativas que podrían indicar actividades sospechosas, como intentos de acceso inusuales, transferencias de datos fuera del horario habitual o el uso de aplicaciones que el usuario normalmente no utiliza. Estas anomalías son frecuentemente un indicador de amenazas internas, como empleados malintencionados, o de cuentas comprometidas por actores externos.

El análisis de comportamiento mediante AA utiliza técnicas avanzadas como el aprendizaje no supervisado, que permite a los modelos detectar anomalías sin necesidad de ejemplos previos de actividades maliciosas. De esta manera, se pueden identificar amenazas emergentes y tácticas novedosas de los atacantes que no están contempladas en los métodos tradicionales basados en firmas.

Inteligencia de Amenazas con Aprendizaje Automático

El uso de aprendizaje automático (AA) ha transformado la inteligencia de amenazas, permitiendo a las organizaciones recopilar y analizar datos de manera más eficiente y efectiva. Los algoritmos de AA mejoran la capacidad para identificar patrones ocultos y correlaciones en grandes volúmenes de datos provenientes de diversas fuentes, como registros de eventos, bases de datos de malware, redes sociales, foros de hackers y plataformas de intercambio de inteligencia de amenazas (TTPs).

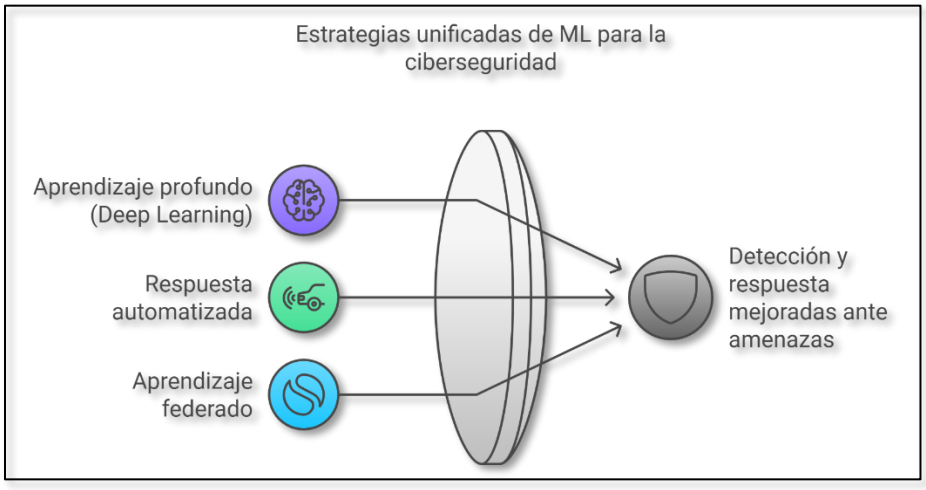
Mediante el análisis continuo de estas fuentes, el AA puede identificar indicadores tempranos de compromiso (IoCs), detectando amenazas emergentes antes de que se conviertan en un problema significativo. Los modelos predictivos aplicados a la inteligencia de amenazas permiten anticipar posibles ataques analizando las tácticas, técnicas y procedimientos (TTPs) utilizados por actores maliciosos en campañas previas. Esto facilita a las organizaciones adoptar una postura más proactiva, implementando contramedidas antes de que las amenazas se materialicen (Tenorio, 2024).



Tendencias

El avance del aprendizaje automático (AA) en ciberseguridad ha dado lugar a nuevas metodologías y enfoques innovadores que están transformando la detección y respuesta a amenazas.

- **Aprendizaje profundo:** El uso de técnicas de aprendizaje profundo, en redes neuronales, ha demostrado ser prometedor para mejorar la precisión de la detección y clasificación de amenazas. Gracias a su capacidad para analizar grandes volúmenes de datos y encontrar patrones complejos, esta técnica permite identificar amenazas avanzadas que podrían pasar desapercibidas con métodos tradicionales(Quirumbay Yagual et al., 2022).
- **Respuesta automatizada:** El aprendizaje automático se está integrando cada vez más en los sistemas de respuesta automatizada, lo que permite a las organizaciones responder a las amenazas en tiempo real sin intervención humana. Esta automatización agiliza la mitigación de incidentes, minimizando el impacto y reduciendo el tiempo de respuesta.
- **Aprendizaje federado:** Este enfoque permite a las organizaciones colaborar en modelos de aprendizaje automático sin compartir datos confidenciales, lo que mejora la privacidad y las capacidades de detección de amenazas. Al distribuir el proceso de entrenamiento del modelo entre múltiples entidades, se logra una mayor precisión sin comprometer la seguridad de la información sensible. Estos desarrollos muestran el potencial del AA para proporcionar soluciones avanzadas y efectivas en el campo de la ciberseguridad.



Soluciones actuales

En el contexto actual de ciberseguridad, el aprendizaje automático (AA) se ha convertido en una herramienta esencial para la protección de infraestructuras y datos críticos. Las soluciones basadas en AA permiten a las organizaciones detectar amenazas complejas y responder a incidentes con mayor precisión y velocidad. La siguiente tabla presenta una selección de herramientas líderes que implementan tecnologías de AA en diferentes enfoques de protección, desde el monitoreo de redes hasta la seguridad en la nube. Cada una de estas soluciones utiliza algoritmos avanzados para identificar comportamientos anómalos, analizar datos de amenazas y mejorar la capacidad de respuesta ante ataques emergentes, proporcionando una defensa integral y adaptativa ante el panorama de ciberamenazas en constante evolución.

Tabla 1.

Soluciones tecnológicas que incorporan AA

Solución	Enfoque de Protección	Descripción	URL
Darktrace	Monitoreo de redes	Utiliza algoritmos de aprendizaje automático para identificar comportamientos anómalos en el tráfico de red, detectando posibles amenazas como malware y ataques de phishing.	https://www.darktrace.com/
IBM Watson for Cyber Security	Análisis de amenazas	Emplea inteligencia artificial para analizar datos de seguridad, identificar patrones y proporcionar recomendaciones de respuesta a incidentes de manera automatizada.	https://www.ibm.com/security/artificial-intelligence
CrowdStrike Falcon	Protección de endpoints	Ofrece protección de endpoints basada en la nube, utilizando modelos de AA para detectar amenazas avanzadas, incluyendo malware y ransomware.	https://www.crowdstrike.com/
Sophos Intercept X	Detección y análisis de malware	Utiliza técnicas de aprendizaje automático para identificar patrones de malware, proporcionando protección avanzada contra nuevas variantes y amenazas emergentes.	https://www.sophos.com/en-us/products/intercept-x
Microsoft Azure Sentinel	Seguridad en la nube	Plataforma de seguridad en la nube que aplica modelos de AA para analizar eventos de seguridad y correlacionar datos de múltiples fuentes, detectando amenazas complejas en tiempo real.	https://azure.microsoft.com/en-us/services/azure-sentinel/
Palo Alto Networks Cortex XDR	Detección y respuesta extendida (XDR)	Combina datos de múltiples fuentes para detectar y responder a amenazas avanzadas, utilizando aprendizaje automático para identificar patrones anómalos y correlacionar eventos de seguridad.	https://www.paloaltonetworks.com/cortex/cortex-xdr

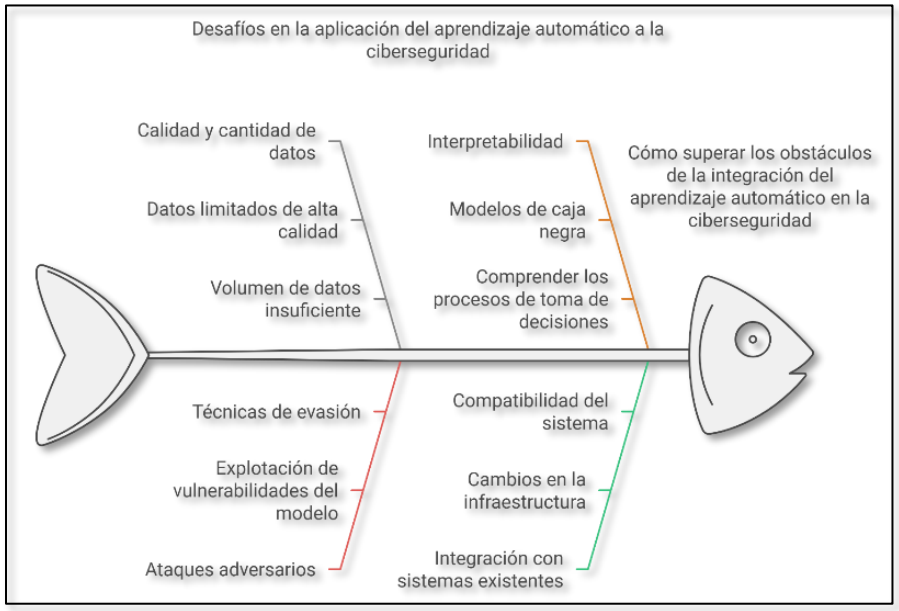
FireEye Helix	Gestión de información y eventos de seguridad (SIEM)	Plataforma que integra inteligencia de amenazas y aprendizaje automático para proporcionar una visión unificada de la seguridad, facilitando la detección y respuesta a incidentes en tiempo real.	https://www.fireeye.com/solutions/helix.html
Vectra AI	Detección y respuesta en la red (NDR)	Utiliza aprendizaje automático para monitorear el tráfico de red y detectar comportamientos sospechosos, enfocándose en identificar amenazas internas y externas antes de que causen daño.	https://www.vectra.ai/
CylancePROTECT	Protección de endpoints	Emplea modelos predictivos basados en aprendizaje automático para prevenir la ejecución de malware en endpoints, incluso sin necesidad de actualizaciones constantes de firmas.	https://www.blackberry.com/us/en/products/cylance-endpoint-security
Rapid7 InsightIDR	Detección y respuesta de intrusiones	Combina análisis de comportamiento de usuarios y entidades (UEBA) con aprendizaje automático para identificar actividades anómalas y potenciales amenazas dentro de la organización.	https://www.rapid7.com/products/insightidr/

Retos

El uso del aprendizaje automático (AA) en ciberseguridad ha demostrado ser una poderosa herramienta para mejorar la detección y respuesta a amenazas. Sin embargo, su implementación presenta varios desafíos que deben abordarse para maximizar su efectividad.

- **Calidad y cantidad de datos**: Los modelos de AA efectivos requieren grandes cantidades de datos de alta calidad, lo que representa un reto en ciberseguridad debido a la escasez de datos etiquetados y la variabilidad de las amenazas. Es de anotar poco a poco las organizaciones viene trabajando en mejorar los procesos de etiquetado de datos y que para optimizar este proceso se puede hacer uso de software especializado para tal fin.
- **Ataques adversarios**: Los cibercriminales pueden explotar vulnerabilidades inherentes a los modelos de AA mediante técnicas de ataque adversario, diseñadas específicamente para manipular los datos de entrada y evadir la detección.
- **Interpretabilidad:** Muchos modelos de AA, especialmente aquellos basados en aprendizaje profundo, funcionan como "cajas negras", lo que dificulta la comprensión del proceso de toma de decisiones para los profesionales de la seguridad, afectando la confianza y la capacidad de respuesta (Hardvard Deusto, 2023).

- **Integración con sistemas existentes**: La incorporación del AA en los marcos de ciberseguridad ya implementados puede ser un proceso complejo, que a menudo requiere ajustes significativos en la infraestructura y compatibilidad con las herramientas actuales. Estos desafíos resaltan la necesidad de desarrollar enfoques sólidos y estrategias adecuadas para la implementación efectiva del aprendizaje automático en el ámbito de la ciberseguridad.



Propuestas con Aprendizaje Automático

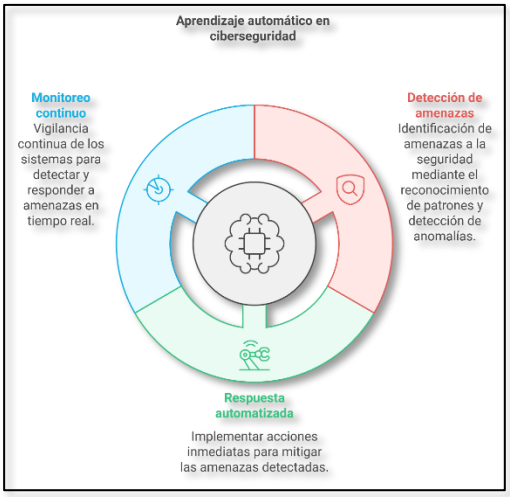
El aprendizaje automático (AA) ha revolucionado el campo de la ciberseguridad, proporcionando herramientas avanzadas que permiten a las organizaciones detectar y responder a amenazas de manera más eficiente y precisa.

Controles de Seguridad:

Detección de amenazas: Los algoritmos de AA pueden analizar grandes cantidades de datos para identificar patrones y anomalías que puedan indicar una amenaza de seguridad.

Respuesta automatizada: La incorporación del AA en los controles de seguridad permite respuestas automatizadas a las amenazas detectadas (*El futuro del aprendizaje automático en la ciberseguridad - Palo Alto Networks*, s. f.).

Monitoreo continuo: El AA facilita el monitoreo continuo del tráfico de red y el comportamiento de los usuarios, lo que permite el análisis en tiempo real y la detección de amenazas (SkyOne Solutions, 2023).

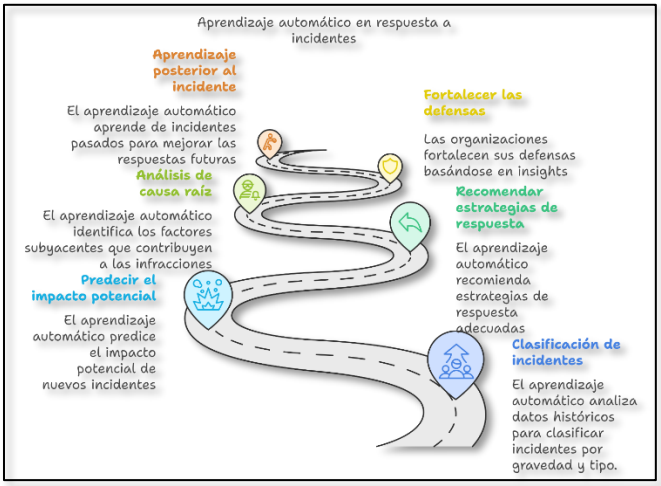


Mejora de la Respuesta a Incidentes

Clasificación de incidentes: El AA puede clasificar los incidentes según su gravedad y tipo, lo que permite a los equipos de seguridad priorizar esfuerzos de respuesta.

Análisis de la causa raíz: Después de que ocurre un incidente, el AA puede analizar la causa raíz al identificar los factores subyacentes que contribuyeron a la infracción.

Aprendizaje posterior al incidente: Los sistemas de AA pueden aprender de incidentes pasados para mejorar las respuestas futuras.



Conclusiones

El estado actual del aprendizaje automático (AA) aplicado a la ciberseguridad demuestra un avance significativo en la capacidad de las organizaciones para detectar y responder a amenazas complejas en tiempo real. Tal como lo destaca el informe del CCN-CERT (2023), la integración de inteligencia artificial y aprendizaje automático permite anticiparse a las tácticas de los atacantes, mejorando la precisión en la identificación de amenazas y reduciendo el tiempo de reacción ante incidentes. Los desarrollos recientes, como el aprendizaje profundo y el aprendizaje federado, muestran un potencial transformador al facilitar el análisis de grandes volúmenes de datos y permitir la colaboración interinstitucional sin comprometer la privacidad de la información. A pesar de los desafíos asociados, como la necesidad de datos de alta calidad y la interpretabilidad de los modelos, Esta revisión ha evidenciado que el uso de estas tecnologías representa una evolución crucial en la ciberseguridad, Promoviendo la adopción de soluciones más adaptativas y proactivas. Con un enfoque en la mejora continua y la implementación de buenas prácticas, como se sugiere en el informe del CCN-CERT, las organizaciones podrán enfrentar con mayor eficacia el cambiante panorama de amenazas, fortaleciendo su postura de seguridad en un entorno digital cada vez más sofisticado y complejo. Por lo anterior, se considera:

- El estado del arte del aprendizaje automático en ciberseguridad está evolucionando rápidamente y ofrece soluciones innovadoras para combatir el creciente panorama de amenazas.
- Si bien persisten los desafíos, el potencial del aprendizaje automático para mejorar las medidas de seguridad y la detección de amenazas es innegable.
- A medida que las organizaciones sigan adoptando estas tecnologías, la investigación y el desarrollo continuos serán cruciales para abordar los desafíos y maximizar los beneficios del aprendizaje automático en ciberseguridad (CCN-CERT, 2023).

Alternativas de herramientas opensource para el aprendizaje automático

Este escenario del AA se viene fortaleciendo de forma progresiva por diversos actores que aportan con soluciones open source a la disciplina de la ciberseguridad y que tiene como fin optimizar a través de herramientas lógicas los procesos de de detección, identificación, contención o respuesta ante eventos o intentos de ataques de ciberseguridad que se presentan en un entorno digital. Este boletín propone a sus lectores el indagar alternativas OSS que contribuyan en la reducción de brechas de seguridad. Para el caso se plantea como herramienta de análisis **packetfence**.

URL de consulta: https://www.packetfence.org/about.html

Algunas características

Aislamiento de Dispositivos en Capa 2:

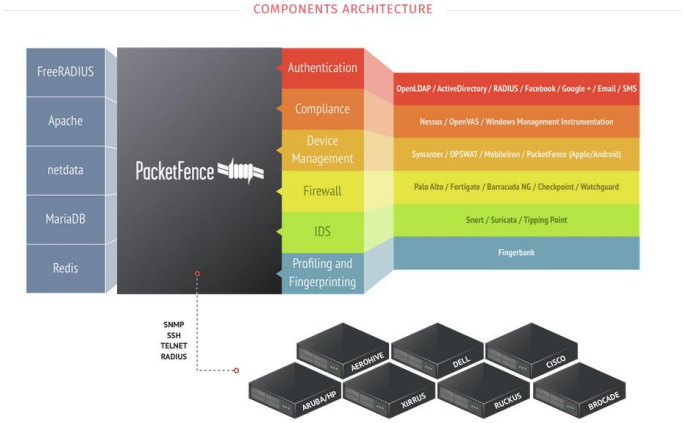
- Aísla dispositivos problemáticos automáticamente para evitar que comprometan la red.
- Utiliza técnicas de segmentación de red para mitigar riesgos.

Integración con Sistemas de Detección de Intrusos (IDS):

- Compatible con herramientas como Snort para detectar intrusiones en tiempo real.
- Ayuda a identificar y mitigar ataques o actividades sospechosas.

Integración con Escáneres de Vulnerabilidades:

- Puede trabajar junto a escáneres como Nessus para identificar vulnerabilidades en dispositivos conectados.
- Mejora la seguridad de la red al detectar y alertar sobre posibles debilidades.



Recuperado de. https://www.packetfence.org/about.html#/overview

Módulos Principales relacionados con AA:

- **Autenticación**: Soporta múltiples métodos.
- **Cumplimiento:** Utiliza herramientas como Nessus y OpenVAS para realizar análisis de cumplimiento de políticas y gestión de vulnerabilidades.
- **Firewall**: Integración con soluciones de firewall como Palo Alto, Fortigate, Barracuda NG, Checkpoint, y Watchguard.
- **IDS**: Soporte para Snort, Suricata y Tipping Point para la detección y respuesta a intrusiones.
- **Perfilado y Huella Digita**: Utiliza Fingerbank para identificar y clasificar dispositivos conectados.

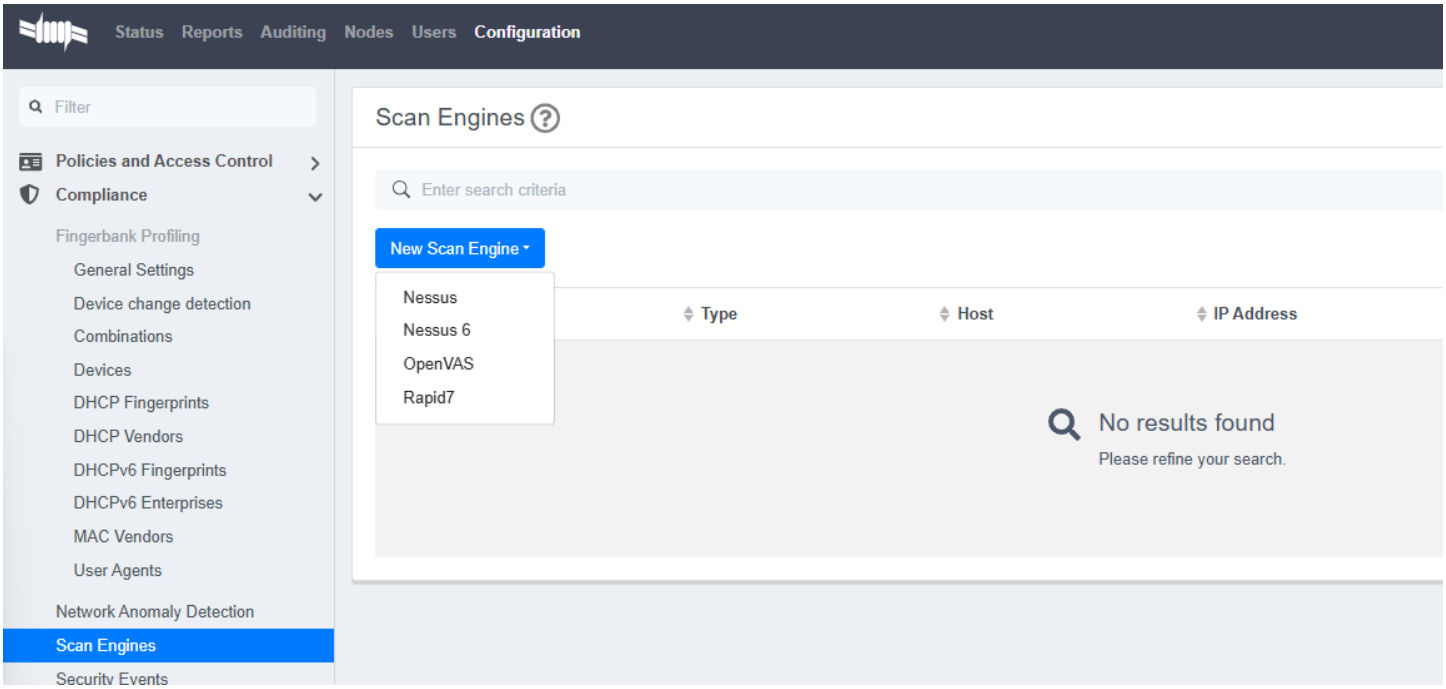


Figura 1. Imagen tomada de aplicación **packetfence**

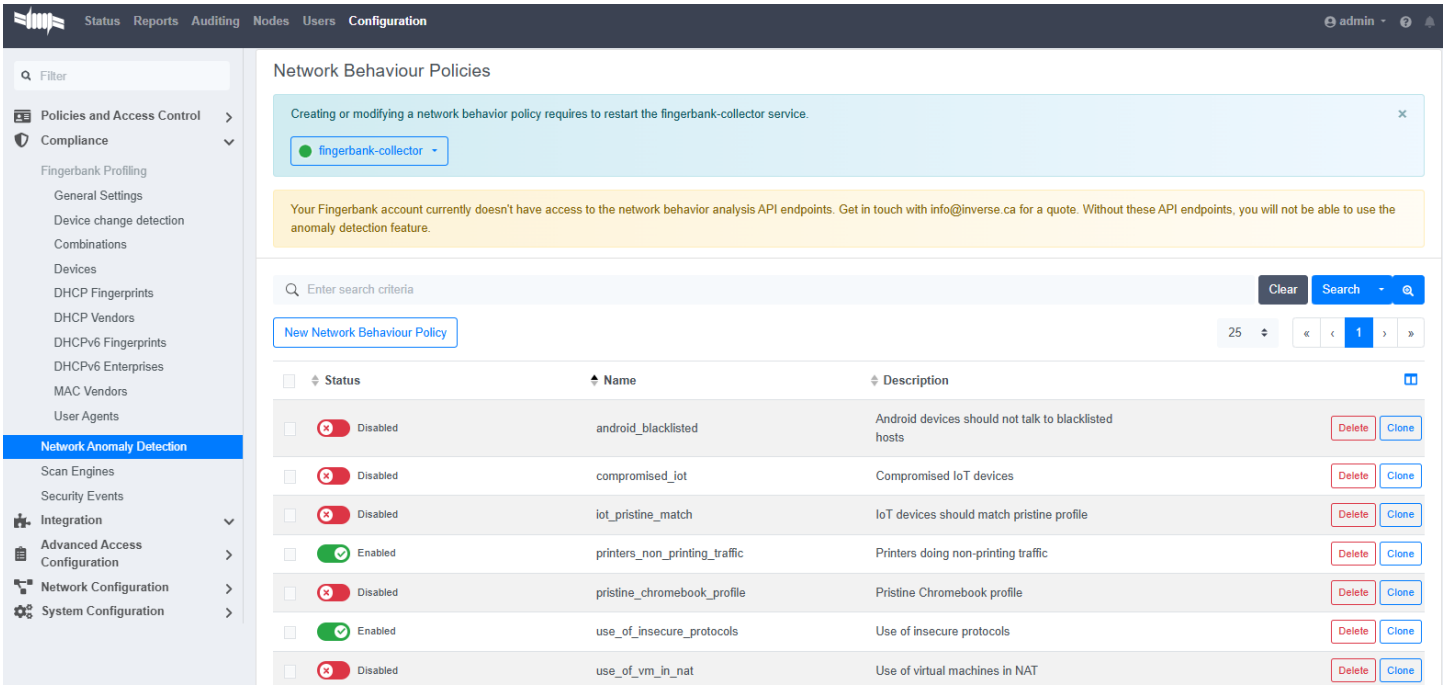


Figura2. Imagen tomada de aplicación **packetfence**

Canales de comunicación

El CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:

- Correo: csirt@unad.edu.co
- Página web: https://csirt.unad.edu.co

Referentes Bibliográficos

CCN-CERT. (2023, octubre 2). *CCN-CERT BP/30 Aproximación a la Inteligencia Artificial y la ciberseguridad*. https://www.ccn-cert.cni.es/es/informes/informes-de-buenas-practicas-bp/7190-ccn-cert-bp-30-aproximacion-a-la-inteligencia-artificial-y-la-ciberseguridad/

El futuro del aprendizaje automático en la ciberseguridad—Palo Alto Networks. (s. f.). Recuperado 15 de noviembre de 2024, de https://www.paloaltonetworks.es/cybersecurity-perspectives/the-future-of-machine-learning-in-cybersecurity

Hardvard Deusto. (s. f.). *El 'machine learning' en la ciberseguridad | Harvard Deusto*. Recuperado 15 de noviembre de 2024, de https://www.harvard-deusto.com/el-machine-learning-en-la-ciberseguridad

Kaspersky. (2020, diciembre 17). *IA y el aprendizaje automático en la ciberseguridad*. /. https://latam.kaspersky.com/resource-center/definitions/ai-cybersecurity

Martín, M. L. M. (s. f.). *Inteligencia Artificial: Un estudio de su impacto en Ciberseguridad*.

Quirumbay Yagual, D. I., Castillo Yagual, C., & Coronel Suárez, I. (2022). Una revisión del Aprendizaje profundo aplicado a la ciberseguridad. *Revista Científica y Tecnológica UPSE*, *9*(1), 57-65. https://doi.org/10.26423/rctu.v9i1.671

Sarker, I. H. (2021). *CyberLearning: Effectiveness Analysis of Machine Learning Security Modeling to Detect Cyber-Anomalies and Multi-Attacks* (Versión 1). arXiv. https://doi.org/10.48550/ARXIV.2104.08080

SkyOne Solutions. (2023). *Aprendizaje automático en ciberseguridad: Automatización de la detección*. https://skyone.solutions/es/blog/aprendizaje-automatico-en-ciberseguridad/