www.vissionfirm.com

NEWSLETTER

Boletín Tecnológico | Ciberseguridad Potenciada por IA y Lucha contra la Desinformación.

¿Qué es?

La **ciberseguridad con IA** utiliza aprendizaje automático, análisis de comportamiento y automatización para detectar amenazas —como malware "polimórfico", phishing sofisticado o ataques de día cero— en tiempo real. En contraparte, la **seguridad contra la desinformación** emplea IA para identificar fake news, deepfakes y redes de bots, tanto en imágenes como en texto o audio.

Lo más relevante

- **Ataques de desinformación aumentan:** campañas como "Operation Overload" están usando IA gratuita para generar contenido falso de forma masiva.
- **Nuevas herramientas defensivas:** soluciones como **Vastav AI** (detección de deepfakes) y **Cyabra** (monitor de desinformación política y empresarial) están ganando presencia.
- **Legislación y colaboración:** Microsoft ofrece apoyo gratuito y hay presión en EU para extender leyes de intercambio de información ciber.

OFICINAS VISSION FIRM

Puebla, Pue.
rgarcia@ vissionfirm.com

Cd. de México.
lcamara@ vissionfirm.com

Guadalajara, Jal.
mcamposllera@ vissionfirm.com

León, Gto.
gpriego@vissionfirm.com

Celaya, Gto.
rgomez@ vissionfirm.com

Querétaro, Qro.
gpriego@vissionfirm.com

Veracruz, Ver.

Contacto:
contactofiscal@vissionfirm.com

Aplicación en el día a día

- **Empresas y gobiernos** integran SIEM y SOAR con IA para respuesta automatizada y priorización de alertas.

- **Protección personal:** sistemas identifican correos fraudulentos, análisis de lenguaje y detectores de deepfake en tiempo real.

- **Conciencia ciudadana:** herramientas monitorizan redes para detectar bots y narrativas falsas rápidamente.

Consejos prácticos

Para organizaciones**:**

- Implementa políticas **zero-trust** con IA, verificando usuario, dispositivo y contexto en cada acceso.
- Usa detectores de deepfake como **Vastav AI** y plataformas como **Cyabra**
- Emplea IA para simulaciones proactivas de ataques y detección de vulnerabilidades.
- Mantén equipos humanos que supervisen las alertas y decisiones de la IA.

Para individuos:

- Utiliza contraseñas únicas y autenticación multifactor .
- Verifica la autenticidad de llamadas o mensajes con “safe-words” o preguntas que solo tu contacto sepa.
- Mantén software actualizado y activa antivirus, VPN y filtros de contenido.
- Desarrolla el pensamiento crítico antes de compartir contenido: comprueba fuentes fiables y aprende a distinguir fake news.

Resumen general

La IA está transformando tanto el **ofensivo** (deepfakes, phishing dirigido con IA) como el **defensivo**: detección mejorada, respuesta automática y autenticidad de información. Herramientas como Vastav AI y Cyabra ejemplifican esta evolución. Las mejores prácticas giran en torno a combinaciones de tecnología (IA + zero-trust), supervisión humana y educación continua.

Llamada a la acción

- **Empresas y profesionales:** adopten frameworks de IA en ciberseguridad, incorporen herramientas anti-deepfake y desplieguen arquitecturas zero-trust con supervisión humana.
- **Ciudadanos y empleados:** protejan su entorno digital: contraseña fuerte, MFA, verifica mensajes con safe-words y practica el pensamiento crítico al consumir y compartir contenido.

Ahora es el momento de actuar: una defensa sólida y consciente hoy evita muchos riesgos mañana. ¡Fortalece tu ciberescudo y combate la desinformación YA!