Webinar:
Seguridad en los tiempos de la IA

Presentación

En el último año, el panorama de la ciberseguridad ha sufrido una transformación radical. Según informes globales de IBM y Tech Advisors (2025), los ataques de **phishing han experimentado un incremento asombroso del 1.265%**, impulsados casi exclusivamente por el uso de herramientas de IA generativa. Ya no se trata solo de volumen, sino de una efectividad alarmante: se estima que un correo redactado por IA tiene una **tasa de apertura del 78%**, superando con creces la capacidad de detección del usuario promedio.

El riesgo no proviene únicamente de actores externos. La **Shadow IA** (el uso de herramientas de IA no autorizadas por la empresa) se ha vuelto un fenómeno universal. Datos recientes indican que el **98% de las organizaciones** tienen empleados utilizando IA sin supervisión, y aproximadamente un **38% de ellos admite haber compartido datos confidenciales**, códigos fuente o secretos comerciales en plataformas de chat abiertas. Incidentes como el fraude masivo en Hong Kong, donde se sustrajeron más de **25 millones de dólares** mediante una videollamada de *deepfake* hiperrealista, demuestran que la frontera entre lo real y lo sintético ha desaparecido.

Este webinar está diseñado para líderes y tomadores de decisión que necesitan comprender que la seguridad ya no es solo una responsabilidad técnica, sino un pilar estratégico. A través de un análisis de estos incidentes y de los riesgos invisibles que introducimos en nuestras organizaciones, exploraremos cómo navegar esta nueva era sin comprometer la integridad de nuestro negocio.

Objetivos

Al finalizar el webinar, los asistentes serán capaces de:

- **Identificar** las dualidades de la IA como herramienta de defensa y ataque en el ecosistema empresarial actual.
- **Analizar** cómo la implementación de IA expande la superficie de exposición de la organización ante amenazas externas e internas.
- **Evaluar** los riesgos intrínsecos (sesgos, alucinaciones y privacidad) para tomar decisiones informadas sobre la adopción de herramientas de IA.
- **Dimensionar** el impacto de la "adherencia" o dependencia excesiva en modelos de IA dentro de los procesos críticos de negocio.

Duración

120 minutos (100 minutos de exposición técnica y sensibilización + 20 minutos de espacio interactivo para preguntas y respuestas).

Temario

1. El escenario de doble filo

- **La IA como escudo:** automatización de respuestas, detección de anomalías en tiempo real y análisis predictivo de amenazas.
- **La IA como espada:** generación de malware polimórfico, phishing hiper-personalizado y ataques de ingeniería social a escala masiva mediante *deepfakes* de voz y video.
- **Expansión del terreno:** cómo la integración de IA en flujos de trabajo tradicionales abre nuevas puertas (APIs, Shadow IA y fugas de datos involuntarias).

2. Riesgos intrínsecos - El enemigo interno

- **Sesgos (bias):** cuando la IA hereda prejuicios. El riesgo reputacional y legal de decisiones automatizadas discriminatorias.
- **Alucinaciones:** el peligro de la "verdad sintética". Cómo la confianza ciega en datos generados puede llevar a errores estratégicos catastróficos.
- **Privacidad y confidencialidad:** ¿a dónde van nuestros datos? El riesgo de alimentar modelos públicos con secretos comerciales o datos personales (PII).
- **Adherencia y dependencia:** el riesgo de la pérdida de habilidades humanas y la vulnerabilidad operativa ante la caída o manipulación de los modelos.

3. Estrategias de mitigación y concientización

- **Cultura de seguridad en IA:** pasos iniciales para una implementación segura.
- **Gobernanza:** creación de políticas de uso aceptable y marcos éticos para empleados.

4. Sesión de consultas

- Espacio abierto para resolver dudas específicas y debatir sobre casos de uso planteados por los asistentes.