

Aplicaciones

1

Detección de Amenazas y Análisis de Comportamiento

Uno de los usos más importantes de la IA en ciberseguridad es la detección de comportamientos sospechosos o anómalos dentro de una red. Los sistemas tradicionales de seguridad se basan en firmas conocidas de malware, lo que significa que no pueden detectar nuevas amenazas sin actualizaciones constantes.

2

Prevención y Respuesta a Ransomware

El ransomware es una de las amenazas más peligrosas en la actualidad. Se trata de un tipo de malware que cifra los archivos del usuario y exige un rescate para su liberación. Los sistemas de IA pueden prevenir ataques de ransomware al analizar el comportamiento del malware en tiempo real y bloquear su ejecución antes de que cause daño.

3

Autenticación Inteligente y Seguridad en el Acceso

Las contraseñas tradicionales son vulnerables a ataques de fuerza bruta y phishing. La IA permite mejorar la autenticación mediante biometría, reconocimiento facial y autenticación basada en comportamiento.

Aplicaciones

4

Inteligencia Artificial en la Caza de Amenazas (Threat Hunting)

El Threat Hunting o búsqueda de amenazas es una estrategia proactiva donde los expertos en ciberseguridad buscan posibles amenazas antes de que causen daños.

La IA acelera este proceso al analizar patrones en los registros de actividad de los sistemas e identificar posibles ataques antes de que se ejecuten.

5

Protección de Dispositivos IoT (Internet de las Cosas)

Con el aumento del uso de dispositivos IoT en hogares y empresas, la ciberseguridad se ha convertido en un desafío. Muchos dispositivos IoT tienen vulnerabilidades que pueden ser explotadas por cibercriminales.

```

# FUNCIÓN: Detectar_Personas_en_Imagen(Imagen_Entrada, Modelo_CNN_Pre_entrenado)

# 1. Pre-procesamiento de la Imagen
Imagen_Redimensionada = Redimensionar(Imagen_Entrada, tamaño Esperado_modelo)
Imagen_Normalizada = Normalizar_Valores_Pixeles(Imagen_Redimensionada)
    # Ejemplos: Convertir a escala de grises, ajustar contraste, normalizar valores de 0-255 a 0-1.

# 2. Inferencia con el Modelo de Detección (CNN)
Resultados_Modelo = Modelo_CNN_Pre_entrenado.Predecir(Imagen_Normalizada)
    # El modelo devuelve una lista de posibles detecciones.
    # Cada detección incluye:
    #   - Coordenadas del Bounding Box (caja delimitadora) [x1, y1, x2, y2]
    #   - Clase del Objeto Detectado (e.g., "persona", "coche", "gato")
    #   - Confianza/Probabilidad de la Detección (e.g., 0.95 para "persona")

# 3. Filtrado y Post-procesamiento
Detecciones_Filtradas = []
Para Cada Deteccion en Resultados_Modelo:
    Si Deteccion.Clase == "persona" Y Deteccion.Confianza > Umbral_Minimo (e.g., 0.7):
        Detecciones_Filtradas.Agregar(Deteccion)

# 4. Supresión de No Máximos (NMS - Non-Maximum Suppression)
# Elimina cajas delimitadoras redundantes o superpuestas para la misma persona.
Detecciones_Finales = Aplicar_NMS(Detecciones_Filtradas)

# 5. Visualización (Opcional, para la presentación)
Imagen_Con_Cajas = Dibujar_Cajas_Delimitadoras(Imagen_Entrada, Detecciones_Finales)
Retornar Imagen_Con_Cajas, Detecciones_Finales

```

1. Pre-procesamiento de la Imagen (Preparación)

Esta fase asegura que la imagen de entrada sea compatible con el modelo de IA. Los modelos de Deep Learning requieren un formato específico para funcionar correctamente.

2. Inferencia con el Modelo de Detección (Procesamiento Central)

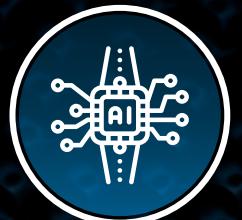
Aquí la inteligencia artificial empezaría hacer un análisis de la imagen, las coordenadas de ella, empezaría analizar los patrones

3. Filtrado y Post-procesamiento (Limpieza Inicial)

Filtrar las predicciones irrelevantes o de baja calidad para reducir el ruido.

Detección de Personas en una Imagen

Principales tipos de IA utilizados en ciberseguridad son:



IA de Grafos (Graph AI)

Analiza las relaciones entre entidades como usuarios, direcciones IP, archivos y procesos. Su objetivo es detectar Amenazas Persistentes Avanzadas (APT) complejas mediante el análisis de cadenas de eventos, construir un grafo de ataque (p. ej., Neo4j + MITRE ATT&CK), un grafo de alcanzabilidad (AM) o la ruta de un atacante, visualizando el movimiento lateral en la red.



Aprendizaje Automático (ML)

El aprendizaje automático (ML) en la ciberseguridad se ha convertido en una herramienta clave para mejorar la detección y respuesta a amenazas ciberneticas. Los algoritmos de ML pueden analizar grandes volúmenes de datos en tiempo real para identificar patrones y comportamientos anómalos que podrían indicar la presencia de amenazas.



Modelos de Lenguaje Grandes (LLM):

Procesa texto no estructurado (informes, correos) para entender el contexto de un incidente. Sin embargo, su uso también plantea desafíos y riesgos que requieren una atención cuidadosa.



CIBERSEGURIDAD

Trabajamos con información, la creamos, la editamos, enviamos, transmitimos, modificamos y eliminamos.

Es vital en nuestros procesos de trabajo y por ello estamos obligados a protegerla, somo el principal elemento de seguridad para nuestra empresa.

Prevención

Como usuarios debemos estar atentos a posibles amenazas y prevenir futuros errores de seguridad

Localización

Detectar el ataque en tiempo real con un antivirus actualizado. Gestionar vulnerabilidades del software y monitorizar de forma continua para conseguir localizarlo

Reacción

1. Desconectar los equipos de la red
2. Pasar el antivirus
3. Cambiar contraseñas
4. Limpieza del sistema
5. Revisar daños