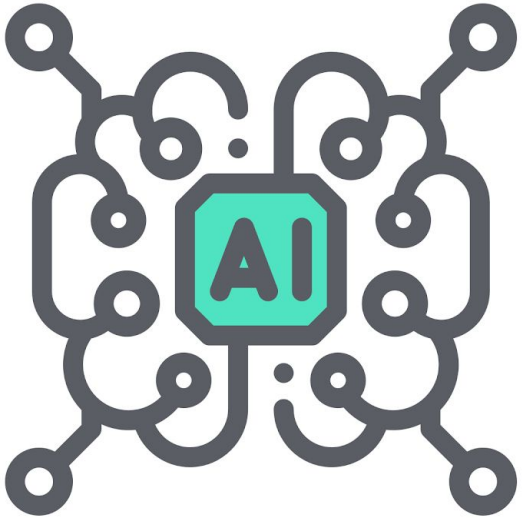
Uso de inteligencia en la **ciberseguridad**



¿Qué usos se le da a la inteligencia en la **ciberseguridad?**

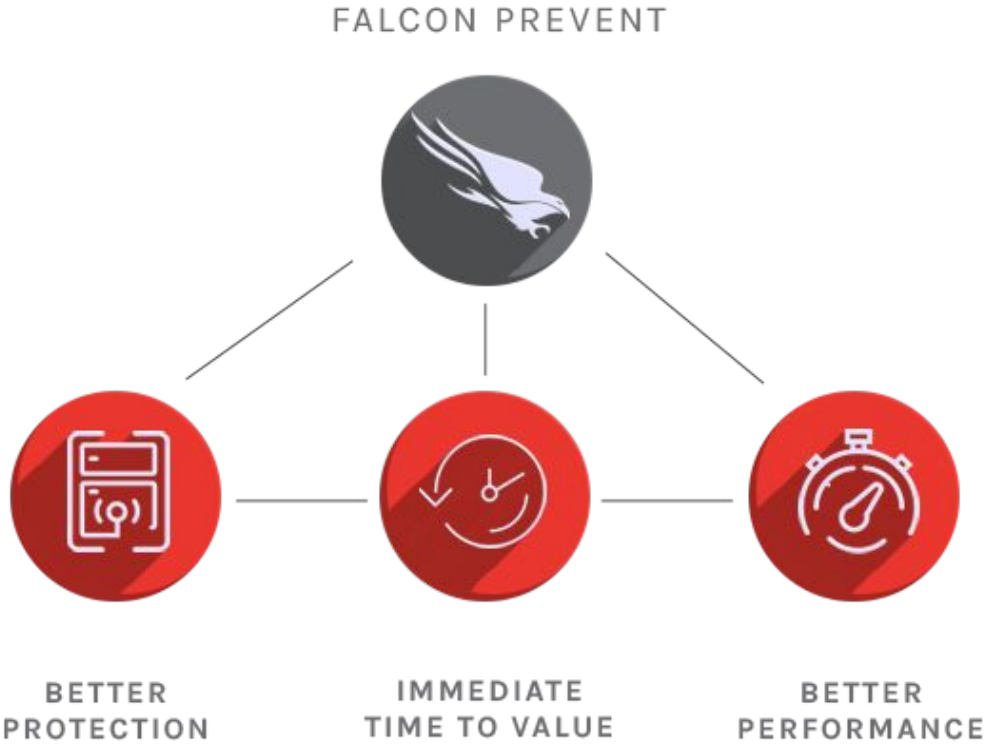
La **inteligencia** ha potenciado tareas de nuestra vida diaria de maneras inimaginables.

Y la ciber-seguridad no es una excepción.

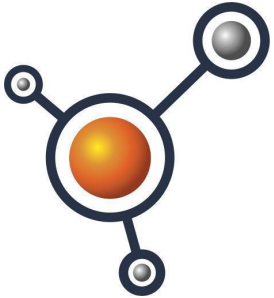
Good

Antivirus

CYLANCE™



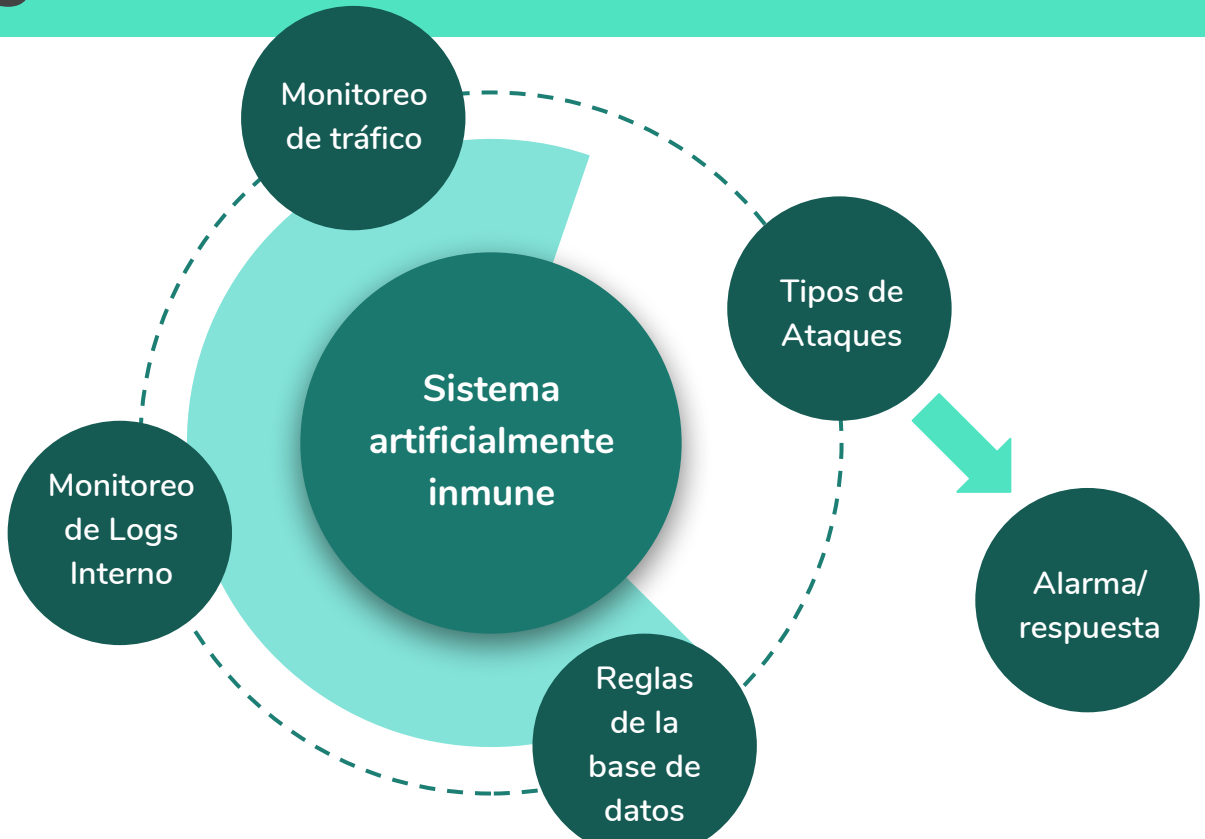
Correlacionadores de eventos



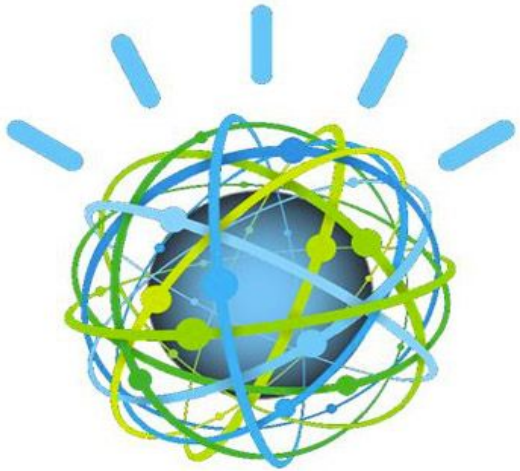
DARKTRACE

splunk>

IDS/IPS


Monitoreo de tráfico
Tipos de Ataques
Sistema artificialmente inmune
Monitoreo de Logs Interno
Alarma/ respuesta
Reglas de la base de datos

(IBM) Watson for cyber security:

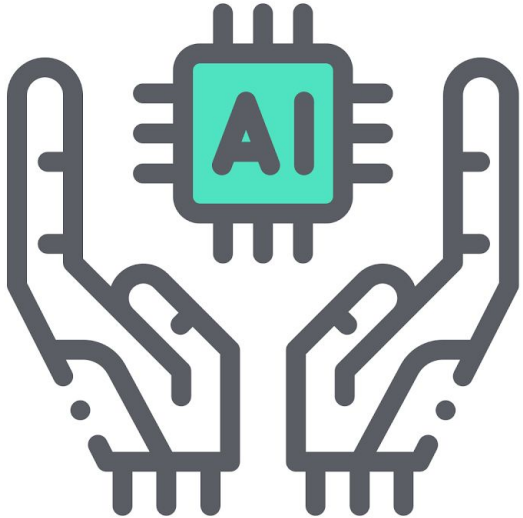


IBM Watson

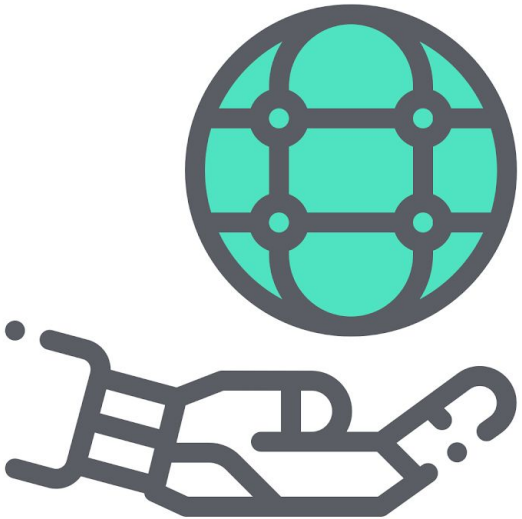
Durante el último año, Watson ha sido entrenado en el lenguaje de la ciberseguridad, asimilando cerca de un millón de documentos de seguridad.

Otros usos

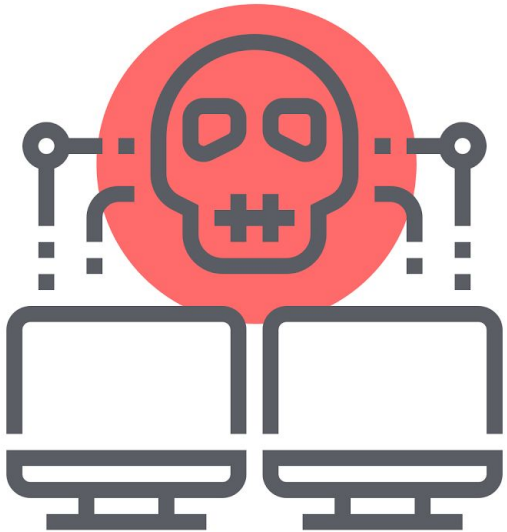
- Análisis de Malware.
- Filtros anti spam.
- Detección de fraudes.
- Detección de BotNets.
- Protección de la privacidad.



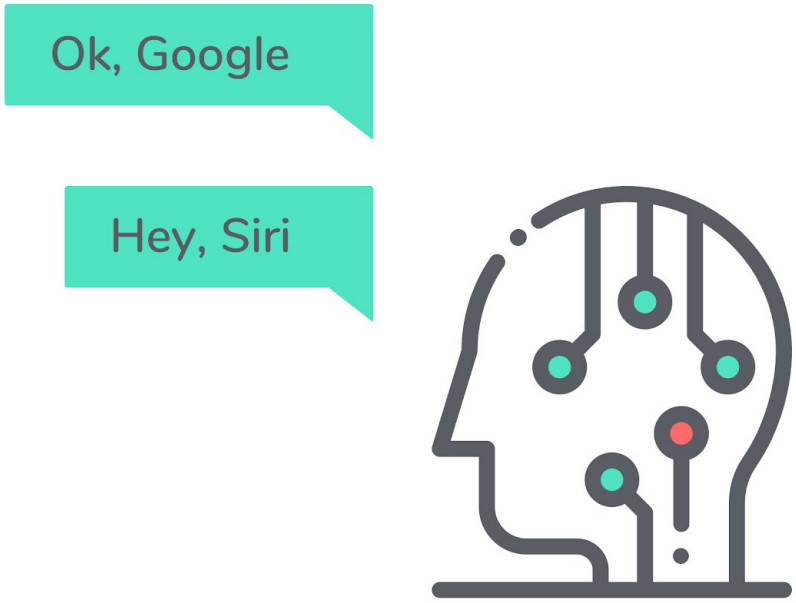
A pesar de todos estos usos benéficos, se le ha prestado poca atención a las maneras en que la inteligencia puede ser usada de manera maliciosa.



Bad



Reconocimiento automático de voz, traducción automática, filtros de spam y motores de búsqueda.



AMAZON'S ALEXA

GOOGLE'S ASSISTANT

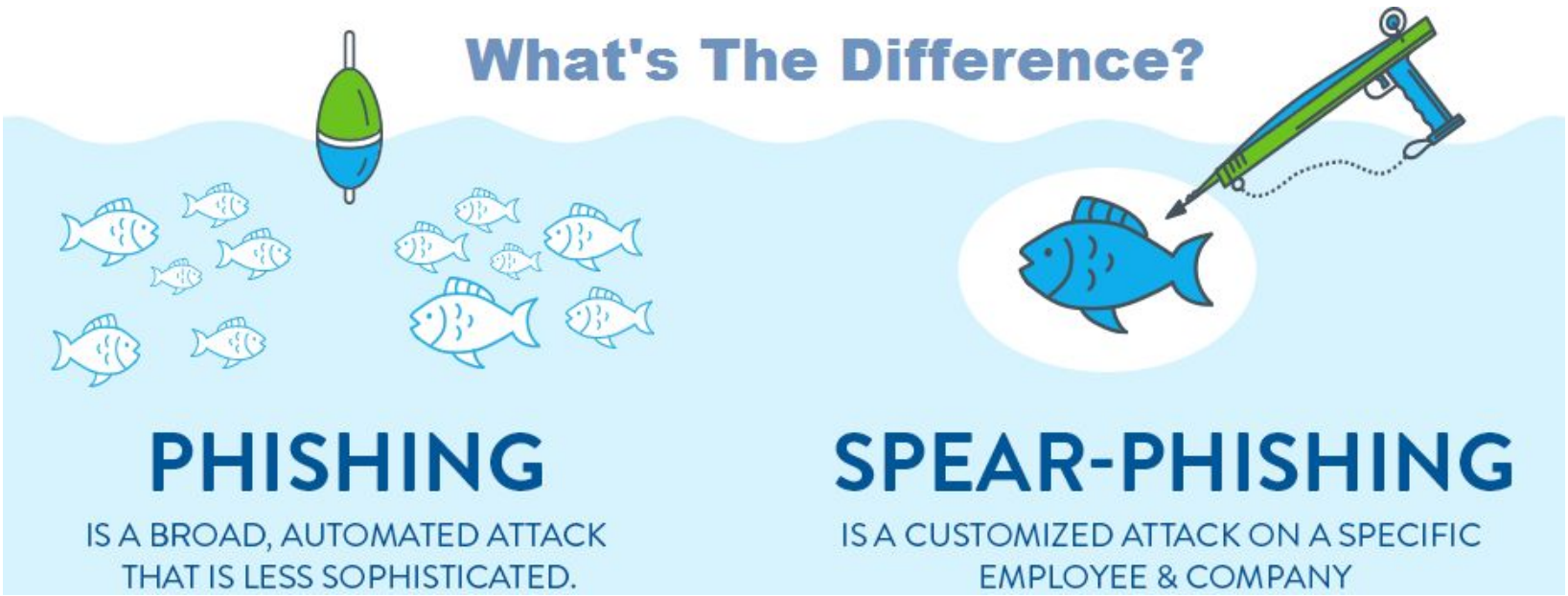
APPLE'S SIRI

MICROSOFT'S CORTANA

Pilotos de pequeña escala que están a prueba: automoviles sin conductor, asistentes digitales y drones habilitados con inteligencia artificial

Seguridad digital

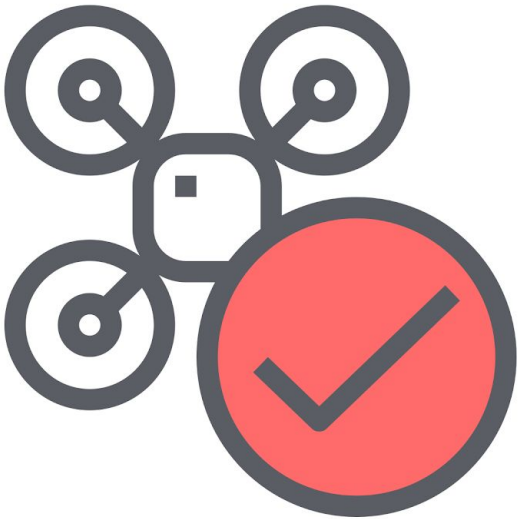
Ciberataques Intensivos



Vulnerabilidades Humanas

Uso de síntesis de voz para la suplantación

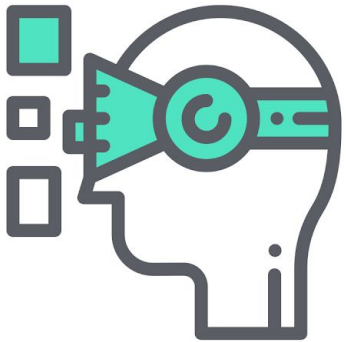
Seguridad física



Drones y otros sistemas físicos

Sistemas físicos que no sería factible dirigir de forma remota (por ejemplo, un enjambre de miles de micro-drones).

¡Pero eso es ficción, es muy futurista!

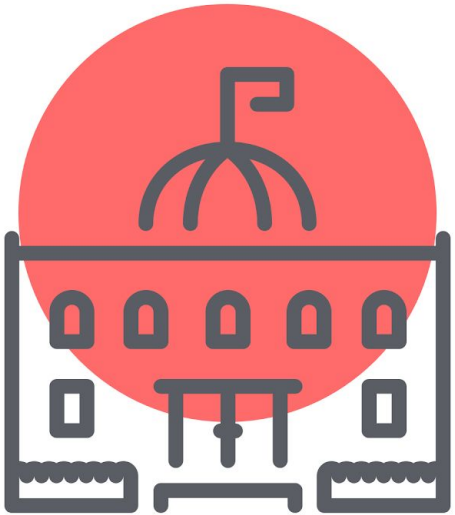


Sí, pero no tanto...

Ataques nuevos que alteran sistemas ciber físicos

Vehículos autónomos.

Seguridad política



Seguridad política.

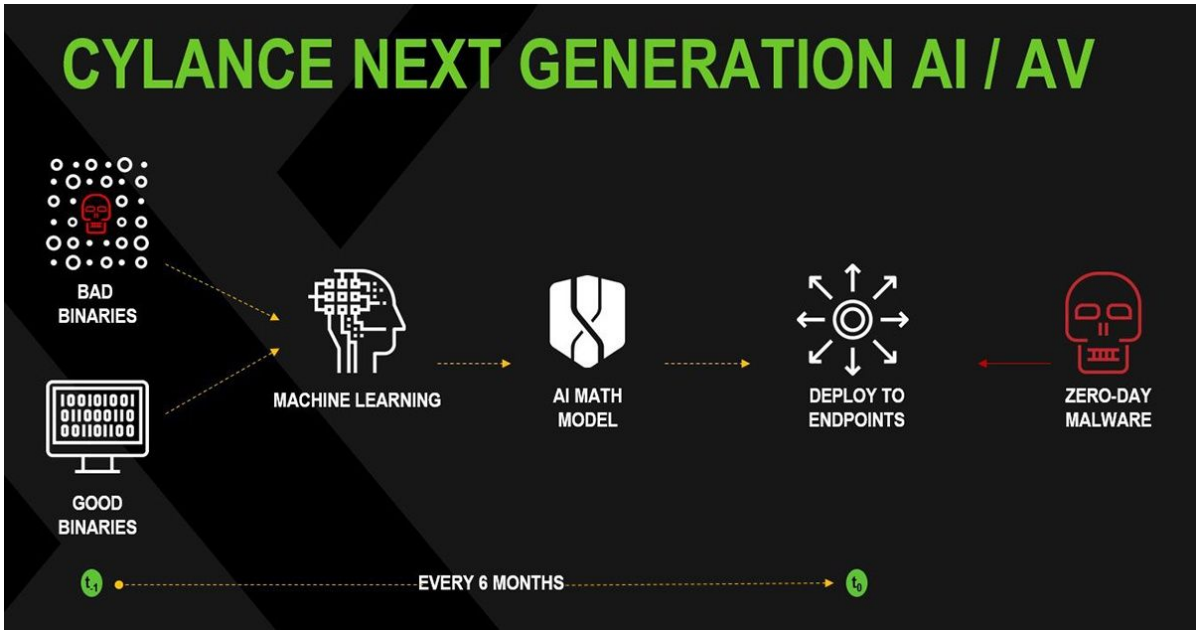
-Vigilancia (por ejemplo, análisis de datos recogidos en masa).

-Engaño (por ejemplo, manipulación de videos).

-Puede expandir las amenazas asociadas con la invasión de la privacidad y la manipulación social.

También se esperan ataques nuevos que aprovechen una mejor capacidad para analizar los comportamientos humanos, los estados de ánimo y las creencias sobre en base a los datos disponibles.

¿Qué pasaría si esto cambiara, se podría crear malware con aprendizaje automático?



En el 2017 en una de las conferencias más grandes de hackers en el mundo, la Defcon, se reveló como crear malware personalizado utilizando el marco OpenAI.

Malware cada vez más evasivo

• La creación de malware suele ser un proceso manual para los ciberdelincuentes.

- Programación de scripts y herramientas (ejecución y propagación)
- ¿El objetivo? Facilitar la distribución y la ejecución.

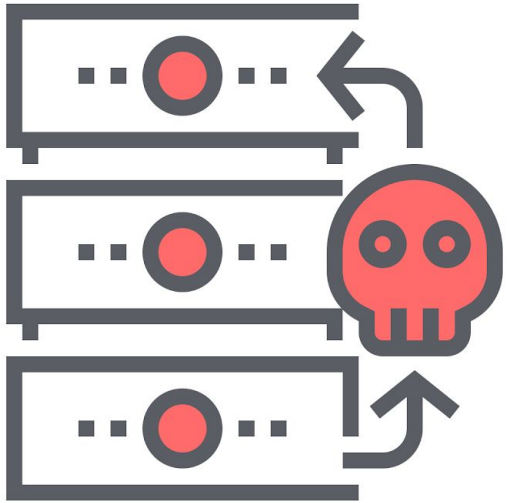
• Evasión de antivirus de próxima generación usando Inteligencia

Malware polimórfico

El malware polimórfico se modifica así mismo.

¿Cómo podríamos acabarlo?

La solución sería hacer lo mismo que el enemigo: cambiar constantemente.



Sin el desarrollo de defensas adecuadas

- Se expandirán las amenazas existentes
- Se introducirán nuevas amenazas
- Se alterará el carácter de las amenazas comúnmente utilizado

El posible costo de los daños por un ciber-ataque pueden ser reducidos por el uso de inteligencia para realizar tareas que normalmente requerirían esfuerzo y experiencia humana.