

# La doble cara de la automatización en Ciberseguridad

Jose Ignacio Viquez Rojas





# Agenda



**01**

La promesa de la automatización

**02**


Desafíos de la automatización

**03**

Caso práctico

**04**

Estrategias para mitigar  
riesgos



# La promesa de la automatización



- Procesar grandes volúmenes de datos
- Identificar patrones anómalos y responder a incidentes
- Integración de diversas fuentes de datos y tecnologías



# Desafíos de la automatización



**Primer desafío:** creciente complejidad del entorno

- Se requiere una arquitectura cuidadosa y una gestión continua para evitar la creación de brechas en la seguridad.
- Los atacantes buscan debilidades en la infraestructura de seguridad y problemas en configuraciones.



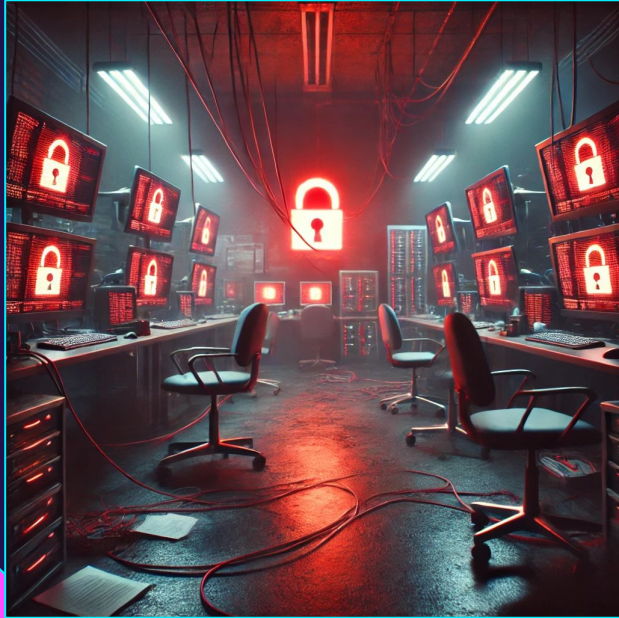
# Desafíos de la automatización



**Segundo desafío:** falta de supervisión humana

- Una automatización puede fallar en escenarios no previstos. Un falso positivo podría resultar en el bloqueo de usuarios legítimos o interrupción de servicios críticos
- La automatización es tan buena como los datos y algoritmos que la alimentan.





## Caso práctico

**Respuesta  
Automatizada a  
un Ataque de  
Ransomware**



# Escenario



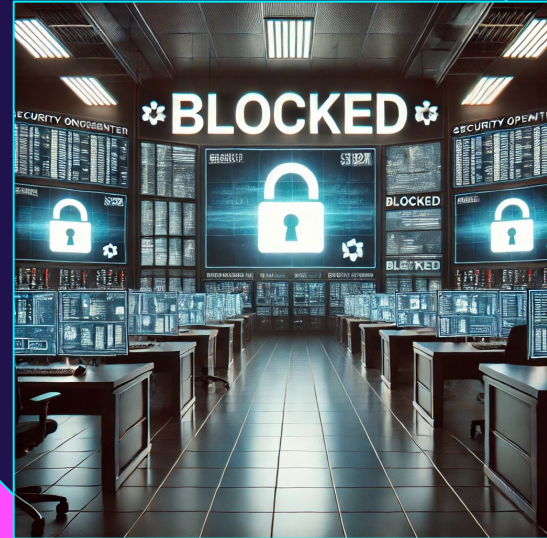
- Una empresa global utiliza un sistema automatizado de detección de intrusiones y respuesta a incidentes para proteger su red.
- El sistema está diseñado para identificar patrones sospechosos y tomar medidas automáticas para mitigar el riesgo.



# Funcionamiento esperado



- Si el sistema detecta un aumento inusual en el tráfico de red, asociado con un proceso de cifrado de archivos el sistema clasifica este aumento como un posible ataque de ransomware.
- Automáticamente bloquea el acceso a la red afectada, generando una alerta.





# Problemas en la automatización



- Sin embargo el tráfico era resultado de una actualización programada en el software de backup de la empresa.
- El sistema automatizado no tenía información actualizada sobre esta operación.
- El sistema bloqueó archivos y servicios críticos, causando una interrupción significativa en la operativa de la empresa.





# Puntos clave



01

## Falta de Contextualización

La automatización no siempre tiene el contexto completo, lo que puede llevar a decisiones erróneas.

02

## Dependencia de Datos Actualizados

Los sistemas deben contar con información y configuración actualizada para evitar errores en la detección.

03

## Necesidad de Supervisión Humana

La intervención humana es crucial para validar y configurar reglas correctas basadas en el contexto extendido de la organización y sus políticas. Así como conocer las integraciones entre distintas herramientas.

# Estrategia para mitigar los riesgos de automatización



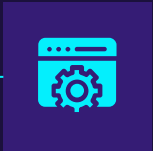
- Mantener una capa de supervisión humana
- Formación continua de los profesionales
- Revisar y ajustar regularmente las reglas y configuraciones para reflejar las nuevas amenazas y el cambio de contextos operativos



# Ideas principales



La implementación de la automatización no está exenta de riesgos.



Habilidad humana para contextualizar y adaptar

