Pentesting en IT y OT

Poniendo a prueba la resiliencia operativa

Dos mundos convergiendo en la cuenca

- La **digitalización** en Vaca Muerta derribó el mito del aislamiento total
- Telemetría remota, sensores IIoT y enlaces cloud conectan las redes de oficinas con pozos, ductos y plantas compresoras
- **El perímetro** ya no termina en el firewall corporativo, puede estar en las redes de control.



Fases de un Pentest en IT



Fase 1: Reconocimiento



Acción: Barrido de superficie de ataque externa, dominios, rangos de IP, credenciales filtradas en Dark Web, servicios cloud expuestos (M365, VPNs).

Objetivo: Encontrar el eslabón débil o credencial corporativa para lograr acceso inicial.



En nuestro caso el reconocimiento externo parte de:

- Relevamiento de activos (sondas, manuales, etc)
- Diagramas de ingeniería (P&ID)
- Ordenes de mantenimiento
- Visitas a campo.

Fase 2: Enumeración



Acción: Nmap agresivo, Nessus/Vulseek con barridos masivos, descubrimiento de servicios, puertos web, RPC, SMB.

Objetivo: Inventariar todo lo vivo y mapear vulnerabilidades conocidas (CVEs).



Acción: es excluyente contar con las versiones de firmware para realizar el assessment correspondiente.

Los protocolos y servicios son y serán siempre los mismos al igual que sus versiones.

Fase 3: Explotación



Acción: Disparo de exploits de memoria, RCE, elevación de privilegios en Active Directory, bypass de defensas (EDR).

Objetivo: Ganar sesión de administración en el servidor o controlador de dominio.



Acción: Solo en laboratorios o gemelos digitales y sobre los protocolos de comunicación, (saber hablar el protocolo, significa poder forzar una bobina o escribir un registro).

Otro tipo de de explotación roza el hardware hacking.

Fase 4: Post-Explotación



Acción: Dump de credenciales (LSASS), movimiento lateral hacia ERP/Finanzas, exfiltración simulada de datos sensibles corporativos.

Objetivo: Comprometer confidencialidad e integridad del negocio administrativo.



No Aplica

Inteligencia Artificial en el Pentesting

¿Autonomía o Ruleta Rusa?



- La esencia del Ethical Hacking
- El problema de los agentes de IA

En producción: La autonomía ciega está prohibida. El pentester humano es quien arbitra el riesgo y cuida la continuidad.

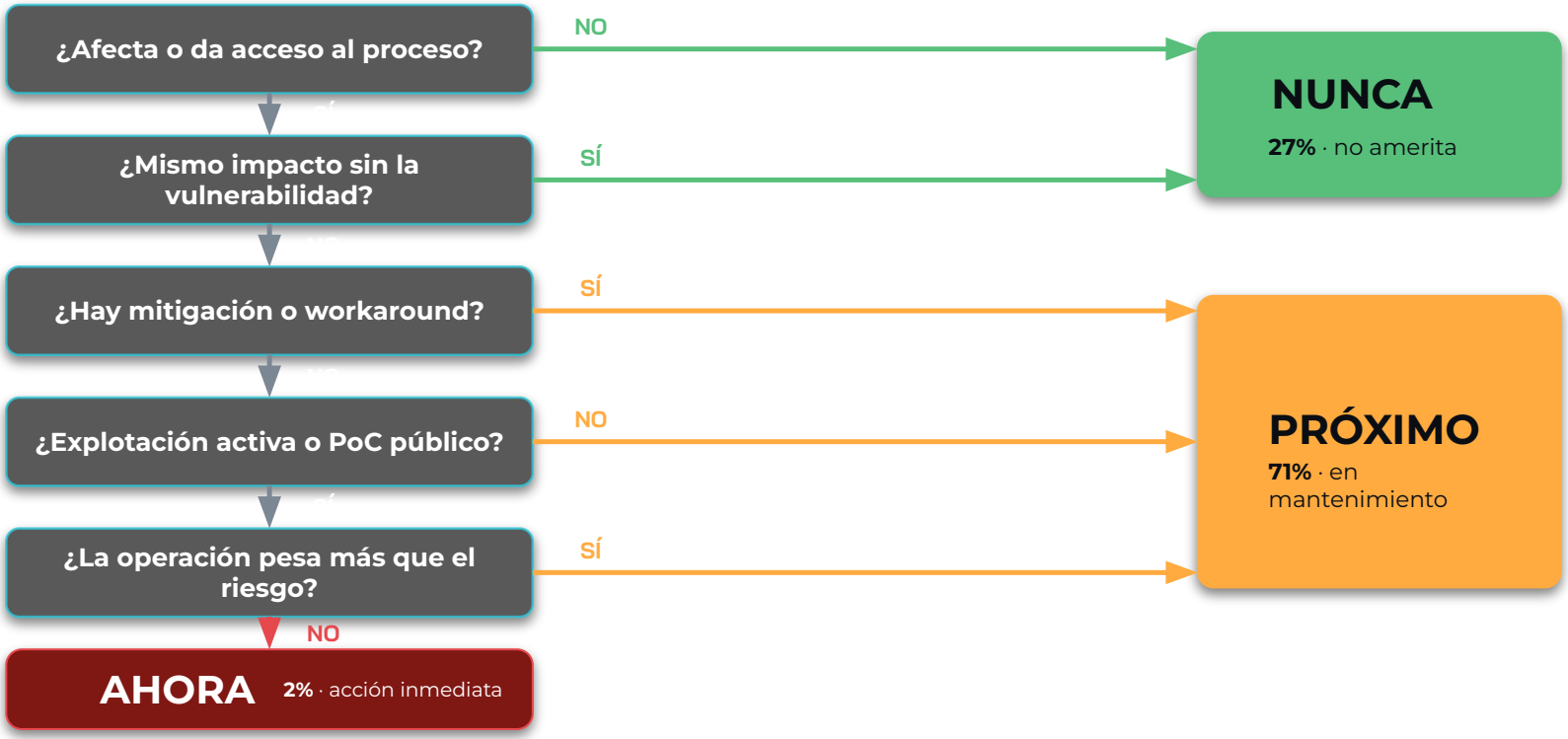
Dónde sí aplica la IA: entornos de laboratorio, controlados, no productivos y con capacidad de rollback inmediato



- El no-determinismo es incompatible con ICS

Dónde sí ayuda en OT: En el entendimiento del proceso para conocer casos de abuso.

Los CVEs en OT realmente aplican?



En IT y en OT compartimos la misma premisa:
El objetivo de un pentest no es demostrar que un sistema se puede romper, sino validar qué tan preparados estamos para proteger la continuidad de la operación.



Vulseek

By Securetia

Vulseek
By Securetia

Securetia

Buscar activo

Español | Solicitar Pentest | Cerrar sesión

Tablero de control

Actualizar cada Desactivado minutos. Última actualización: 08:04:13

Vulnerabilidades por prioridad

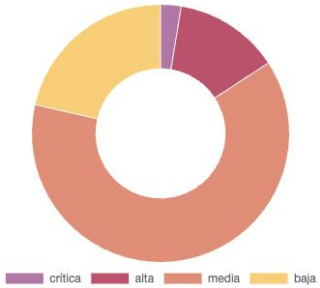
Crítica	Alta	Media	Baja
20	38	73	28

4	25	4	316
Dominios	Hostnames	Direcciones IP públicas	Direcciones IP privadas

Hallazgos por antigüedad

	90+ días	61-90 días	31-60 días	8-30 días	0-7 días
Crítica	18	0	1	3	0
Alta	72	5	11	9	16
Media	260	179	7	26	65
Baja	55	108	1	16	3

Hallazgos por prioridad



Vulseek

- ✓ Simplicidad y rapidez: Detección y gestión de vulnerabilidades
- ✓ Priorización medida por criticidad y probabilidad de explotación
- ✓ El Modelo Híbrido

Vulseek



¿Preguntas?

¡Muchas gracias!



Securetia

Expertos en ciberseguridad

info@securetia.com