

# PENTERA PT AUTOMATIZADO

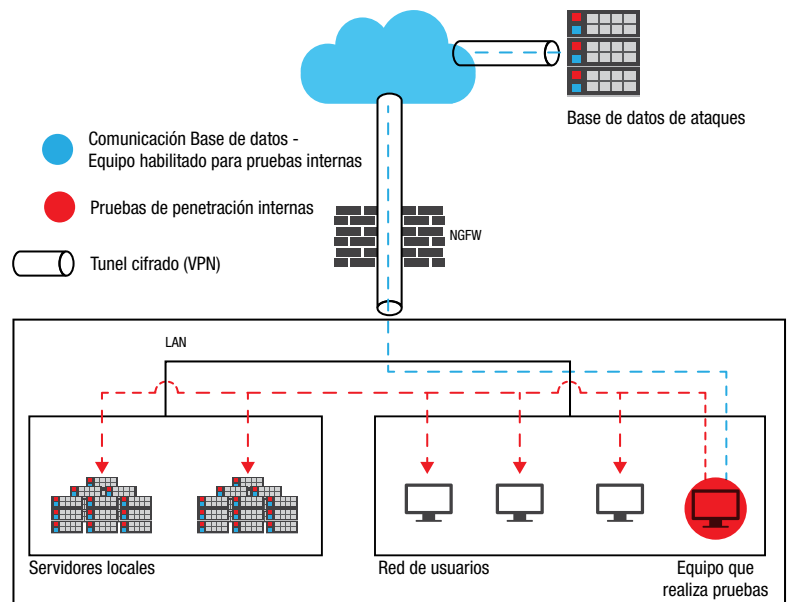


potencia tu información

Con un enfoque en amenazas internas IPTaaS simula a un atacante que ha logrado burlar tus controles de seguridad a través de cualquiera de los vectores y se ha posicionado en tu red, donde desde cero comienza el descubrimiento de vulnerabilidades y amenazas en toda dirección posible (movimientos laterales).

El análisis de IPTaaS analiza a profundidad **cada dispositivo en tu red interna** mientras se asegura de no causar ningún daño o interrupción al no ejecutar ataques invasivos o ataques que tu no hayas autorizado.

Obtén completa visibilidad de todo lo que puede hacer un atacante en tu red para la explotación de vulnerabilidades y robo de información mediante reportes que describen paso a paso vulnerabilidad, impacto, explotación y sobre todo la remediación.



## IPTaaS frente a PT tradicional

### IPTaaS

- Toda tu red interna es el alcance
- Frecuencia continua o bajo demanda
- Primeros resultados en minutos
- Análisis constante y comparativos del tiempo
- Consistencia de ataques: millones de ataques sin parar
- Base de datos de amenazas de nivel mundial
- Proyecto y planeación: Plug and Play (preparación en minutos)
- Mucho más redituable que el PT tradicional
- Requiere un proyecto definido por terceros
- Contiene las últimas vulnerabilidades y amenazas
- Resultados visibles solo para la compañía

### PT Tradicional

- Alcance limitado
- Frecuencia una vez cada 6 o 12 meses
- Resultados en revisiones semanales
- Resultados en una imagen de tiempo
- La consistencia de ataques son limitados por el consultor
- Muy dependiente del talento del consultor
- Un equipo debe ser asignado al proyecto
- Costoso
- Requiere un proyecto definido por terceros
- Sin garantía de que el consultor pueda replicar las últimas amenazas
- Un consultor externo con el conocimiento de tus vulnerabilidades

potencia tu información

## ¿Cómo lo hacemos?

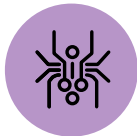
El ejercicio es preparado por nuestro equipo de expertos. Se prepara un dispositivo dentro de la red de la compañía objetivo con una VPN que conectará a nuestros servidores desde donde se mandarían los ataques. Se define la duración del ejercicio y el alcance de éste. Esta preparación toma algunos minutos.

Se definen puntos de control donde, en conjunto con el cliente, se aprobarán algunos ejercicios que pudieran significar algún impacto. No se realiza ningún ejercicio de riesgo del que no se tiene aprobación.

## Beneficios

- **Protección continua.** Mantenga todas sus redes al mismo nivel de protección.
- **Validación constante.** Realice los tests con la frecuencia necesaria: diaria, semanal, mensual.
- **Defensa actualizada.** Manténgase al día con las últimas técnicas del hacking. Los hackers evolucionan constantemente sus técnicas y herramientas, por lo tanto es fundamental que sus herramientas de validación de riesgos evolucionen tan rápido como ellos.
- **Despliegue fácil**

## Características del Producto



### Sin agente

Instalaciones de agente cero o configuración de red. Las pruebas de penetración inician con acceso físico a la LAN sin ninguna credencial. Justo como harían un hacker.



### Acciones Inofensivas

Como los hackers, realizamos explotaciones éticas sin interrumpir el servicio: movimientos laterales, ejecución remota, ataques de retransmisión, robo de contraseñas, penetración de malware y escalada de privilegios.



### Visibilidad del vector de ataque

Cada paso en el ataque del vector es presentado y reportado en un documento detallado y explica el ataque "kill chain" donde se selecciona una mínima cantidad de vulnerabilidades para detenerlo.



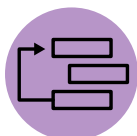
### Automatizado

Dale play y haz tus cosas mientras la prueba de penetración se ejecuta. Lo único que tienes que hacer es definir el rango de IPs y checar el tipo de pruebas que quieres ejecutar.



### Ataca tus puntos de control

Para los sistemas de misión crítica, un oficial de seguridad de la empresa puede asumir un control discreto para etapas de explotación de orden superior para controlar selectivamente el nivel de intrusión del ataque.



### Remediación priorizada

Obtenga un resumen claro de los pasos de remediación críticos a realizar en función de las prioridades de enfrentamiento de amenazas que son relevantes para la red de su organización y los activos críticos.



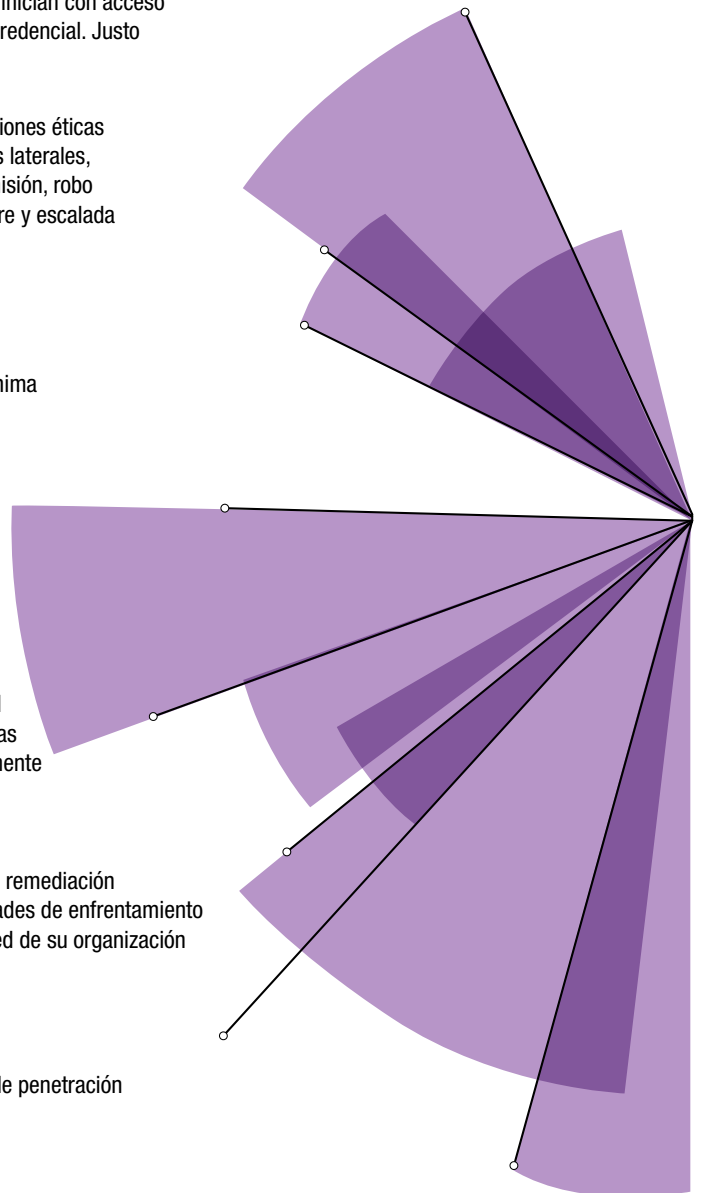
### Las últimas técnicas de hackeo

Las técnicas de las pruebas de penetración son las más actualizadas.

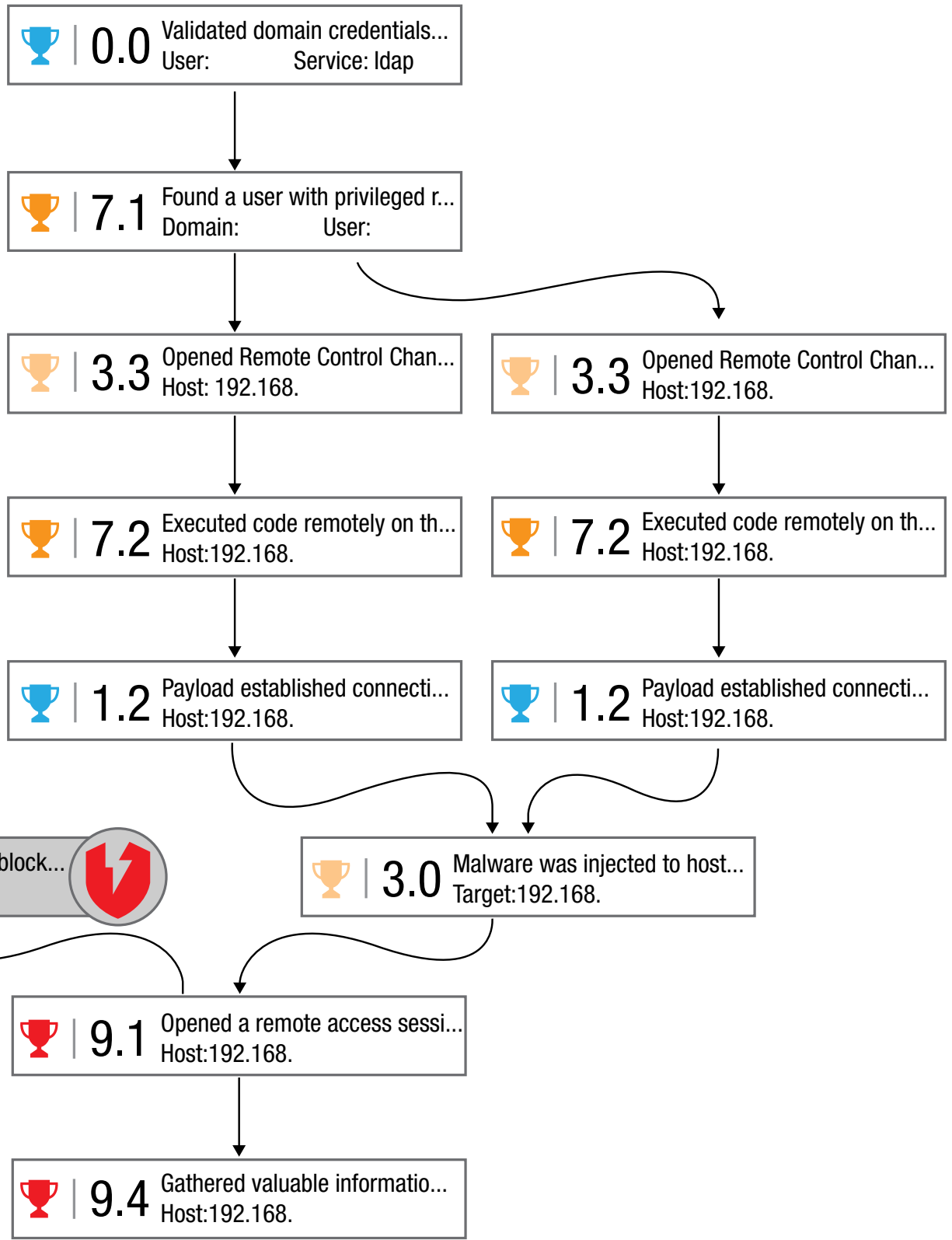


### Alertas comerciales personalizadas

Puede establecer cualquier punto de partida y objetivo de prueba de penetración y ejecutar una prueba de ataque dirigida para una debilidad específica o para la resistencia cibernética de aplicaciones específicas.



Entiende el flujo de una explotación exitosa e identifica dónde está tu punto débil y cómo puedes corregirlo.

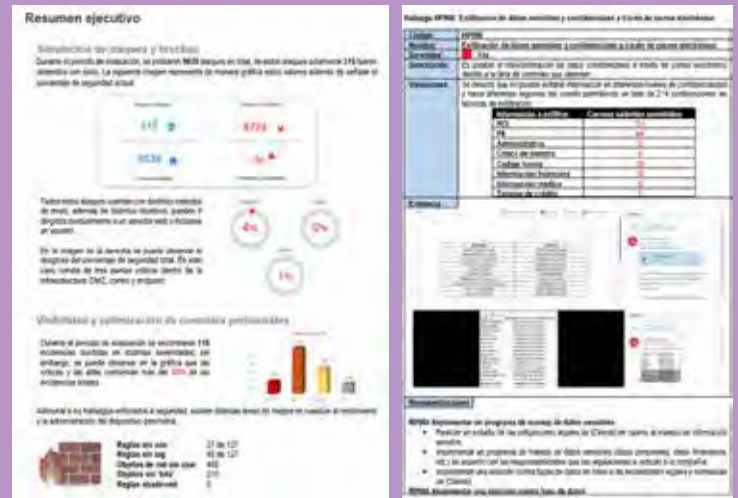
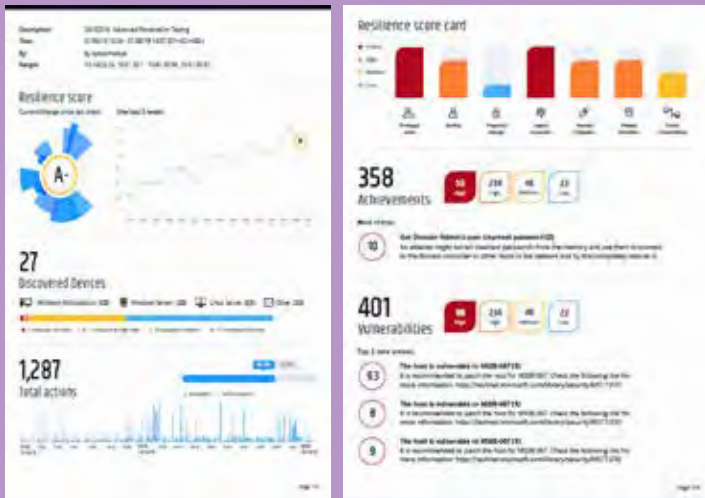


## Resultados

Obtén resultados entendibles y accionables gracias al uso de marcos de trabajo y metodologías conocidas, además de semáforos y KPIs que permitirán trazar correctamente el avance obtenido en un periodo.

La cantidad de IPs y tipos de dispositivos no es un impedimento, como lo es para la oferta de PenTest típicos del mercado. Nuestro servicio es capaz de realizar una prueba de PenTest interno eficiente, ágil y controlada para no afectar a tu organización y entregarte resultados.

Obtén el acompañamiento de nuestro grupo de expertos que ayudarán a traducir los hallazgos y recomendaciones en un plan de acción digerible y eficiente para tu organización.



## Nuestro modelo de servicios

Círculo Daat atendiendo la situación económica global y la dinámica actual de trabajo, considera algunas opciones de servicio que se pueden ajustar a las necesidades particulares de cada uno de nuestros socios de negocio, pudiendo ejecutar las pruebas desde una vez, hasta pruebas continuas con reportes de avances periódicos.

### CENTRO

🏠 Filadelfia 128, Oficina 602  
Col. Nápoles  
Alcaldía Benito Juárez  
México CDMX 03810

### CONMUTADOR

☎️ +52.55.5202 5010  
✉️ comercial@circulodaat.mx  
🌐 [circulodaat.mx](http://circulodaat.mx)

### NORTE

☎️ +52.81.4159 0580  
🏠 Penthouse 1, Edificio III Moll del Valle  
Calzada del Valle 400  
Col. Del Valle  
San Pedro Garza, García