PICUS

Simulación de Intrusión de ataques

Picus Security BAS (Breach and Attack Simulation) es una plataforma que simula ataques del mundo real para validar y mejorar la eficacia de los controles de seguridad de una organización.

Sirve para probar y medir continuamente las herramientas de detección y prevención de amenazas, identificar brechas de seguridad, visualizar rutas de ataque, validar la efectividad de las reglas de detección, y obtener información procesable para optimizar las inversiones en seguridad y fortalecer la resiliencia cibernética

¿Qué hace Picus BAS?

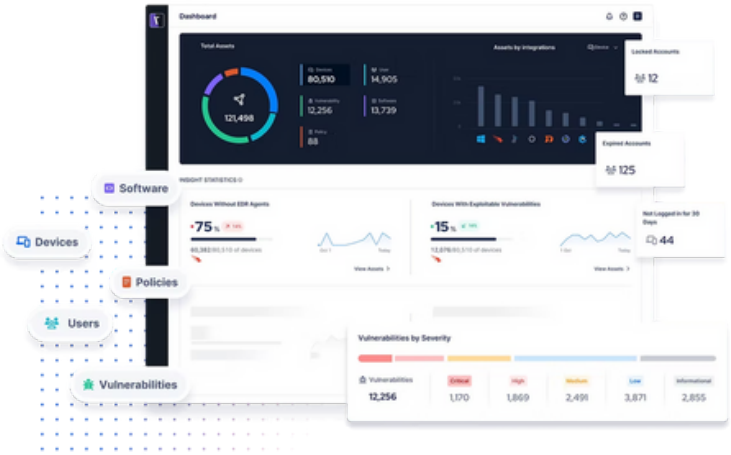
Simula ataques reales: Ejecuta miles de simulaciones de amenazas y técnicas de ataque para verificar si los controles de seguridad funcionan correctamente.

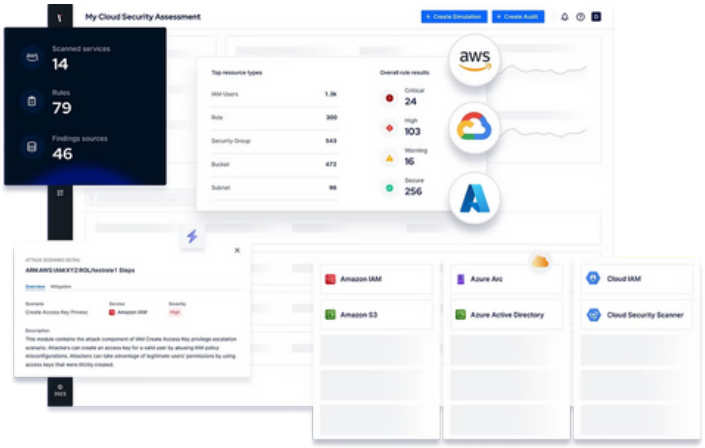
Válida controles de seguridad: Asegura que las herramientas de prevención y detección, como firewalls y sistemas de detección de intrusos, estén bien configuradas y sean efectivas.

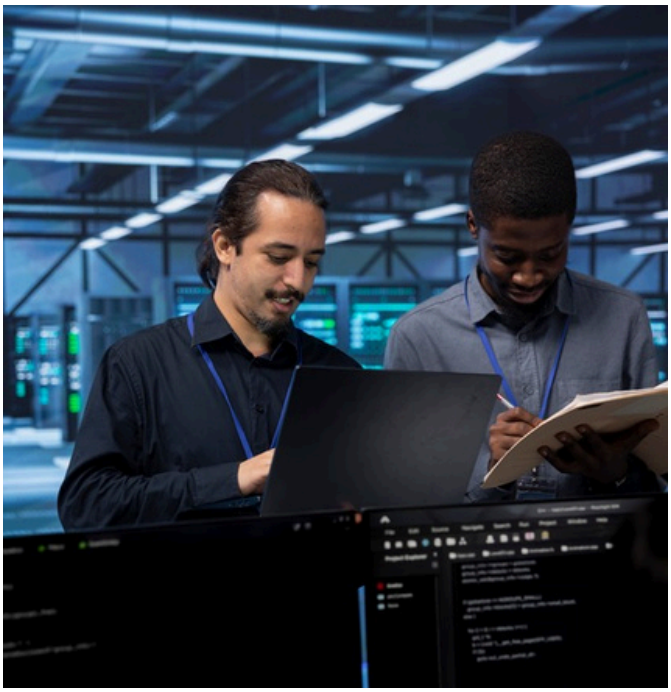
Identifica brechas de seguridad: Permite encontrar vulnerabilidades y configuraciones erróneas en la nube y en el entorno de red antes de que sean explotadas por atacantes.

Valida la efectividad de las reglas de detección: Ayuda a los equipos de seguridad a mantenerse al día con la línea base de sus reglas de detección y automatiza los procesos de ingeniería.

Visualiza rutas de ataque: Muestra los pasos que un atacante podría seguir para comprometer los sistemas, revelando los puntos más críticos para el riesgo







Para qué sirve

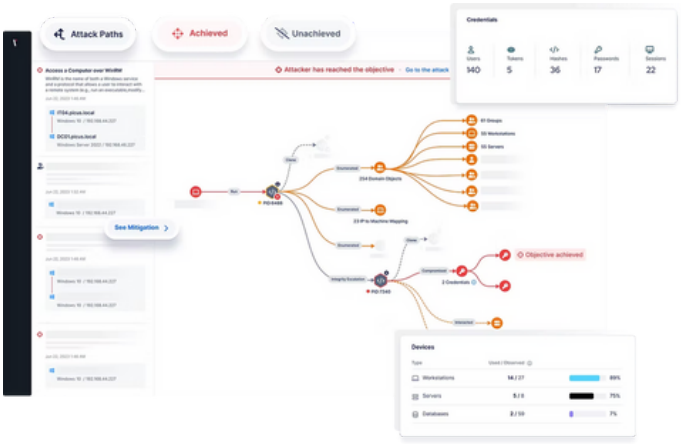
- **Mejora la resiliencia cibernética:** Fortalece la capacidad de una organización para prepararse y recuperarse de ataques cibernéticos.
- **Reduce el riesgo cibernético**: Al identificar y mitigar proactivamente las vulnerabilidades, disminuye la exposición a los atacantes.
- **Optimiza las inversiones en seguridad:** Comprueba el valor de las inversiones realizadas en herramientas de seguridad, asegurando que protegen eficazmente.
- **Aumenta la visibilidad de la postura de seguridad:** Proporciona una visión integral y holística de la seguridad de la organización.
- **Automatiza las pruebas de seguridad**: Libera al personal de la necesidad de realizar pruebas manuales, permitiéndoles enfocarse en brechas críticas y soluciones de alto impacto

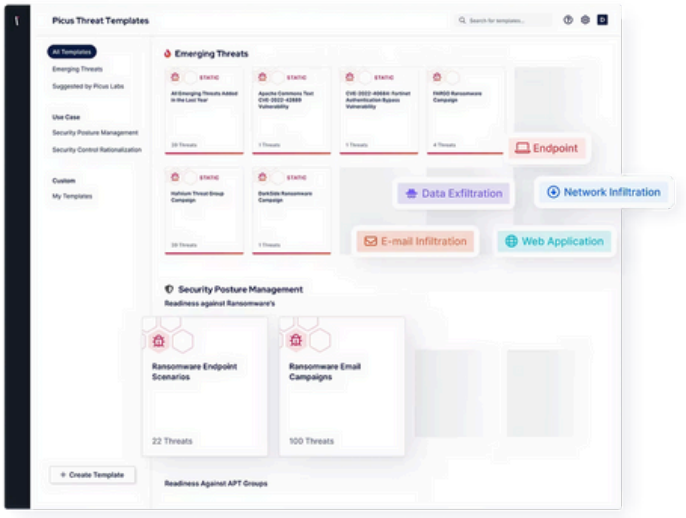
Ejemplo práctico en las empresas

Imagine una empresa de tecnología que ha invertido en varias soluciones de seguridad, incluyendo un firewall de última generación y un sistema de detección y respuesta de puntos finales (EDR). El equipo de seguridad utiliza Picus Security BAS para evaluar la eficacia de estas defensas

1. Simulación de un ataque de ransomware

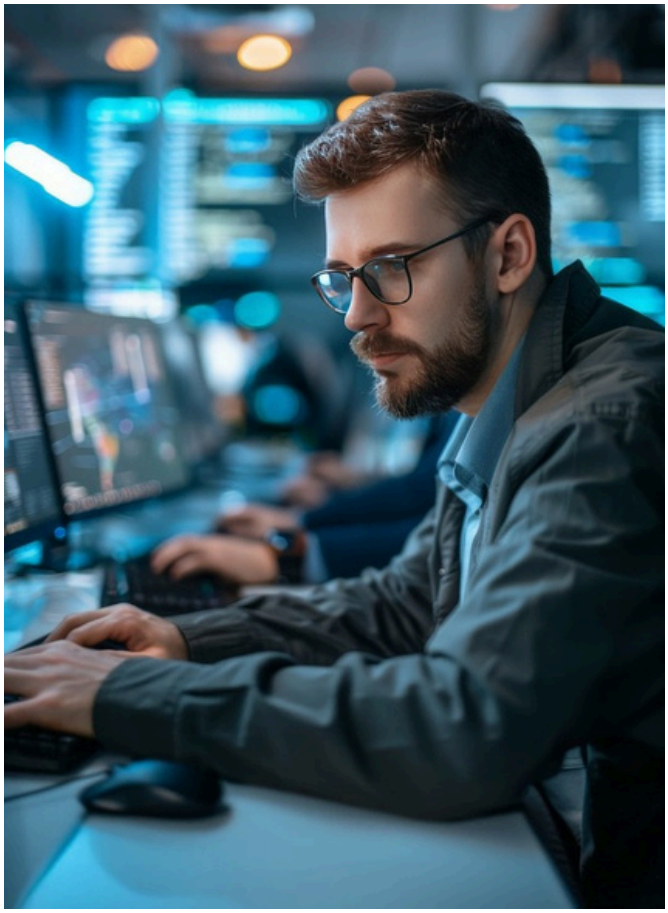
- **Configuración**: El equipo de seguridad de la empresa lanza una simulación de ataque de ransomware a través de la plataforma de Picus. La simulación emula las tácticas que un atacante real utilizaría, como el movimiento lateral, el robo de credenciales y la exfiltración de datos.
- **Ejecución**: Picus despliega pequeños agentes de software (sin riesgo para los sistemas) que actúan como atacantes dentro de la red. Estos agentes intentan evadir las defensas, buscar vulnerabilidades y realizar acciones maliciosas simuladas.
- **Validación de la detección**: El sistema comprueba si el EDR de la empresa detecta los movimientos del atacante simulado y si el SIEM genera alertas apropiadas y oportunas.
- **Validación de la prevención**: Verifica si el firewall bloquea el tráfico malicioso que intenta exfiltrar datos.





2. Análisis de resultados y mitigación

- **Resultados de la simulación**: El informe de Picus revela que, si bien el EDR detectó el ransomware en la fase inicial, no generó una alerta crítica en el SIEM. Además, una configuración incorrecta en el firewall permitió el paso de tráfico de exfiltración simulado.
- **Recomendaciones accionables**: La plataforma proporciona recomendaciones claras, como ajustar la regla de correlación en el SIEM para que las detecciones del EDR generen alertas de alta prioridad. También sugiere corregir la configuración del firewall para bloquear el tráfico de exfiltración



3. Verificación de la mejora

- **Nueva simulación**: Después de implementar las correcciones recomendadas, el equipo ejecuta una nueva simulación de ataque de ransomware.
- **Resultados mejorados:** El informe muestra que, en la segunda prueba, el EDR detectó el ataque, y esta vez el SIEM generó una alerta crítica, lo que permitió al equipo de seguridad responder de manera oportuna. Además, el firewall bloqueó exitosamente el intento de exfiltración de datos

Este ejemplo demuestra cómo Picus BAS permite a las empresas pasar de una postura de seguridad reactiva a una proactiva. En lugar de esperar a ser atacados para descubrir debilidades, las empresas pueden identificarlas y corregirlas de forma continua y automatizada