SIMULACIÓN DE
VULNERABILIDAD Y ATAQUE

EL NUEVO ENFOQUE HACIA LA VALIDACIÓN DE LA SEGURIDAD CIBERNÉTICA

La plataforma de simulación de ciberataques de Cymulate le permite a las empresas probar su nivel de seguridad, identificar posibles vulnerabilidades y recibir información práctica para mejorar su seguridad.

Funciona simulando ataques de múltiples vectores, internos o externos, que incluyen las últimas vulnerabilidades derivadas del departamento de investigación de Cymulate. El resultado es una validación completa de la situación actual de la seguridad de la organización, en el momento que lo necesite y con cero falsos positivos.

CYMULATE

ESTÁ A 7 MINUTOS DE
SABER SI ESTÁ SEGURO!

PRUEBE SU NIVEL DE SEGURIDAD 24/7/365

Las organizaciones ahora tienen el poder de verificar su nivel de seguridad, bajo demanda, a través de una plataforma única de simulación de vulnerabilidades y ataques cibernéticos.

La tecnología avanzada de Cymulate permite a las organizaciones lanzar simulaciones de cíberataques contra ellas mismas, ofreciendo de inmediato las vulnerabilidades y procedimientos de mitigación para cerrar cada brecha.

La plataforma centralizada de Cymulate permite realizar pruebas de seguridad a través de múltiples vectores de ataque, como correo electrónico, navegación, red interna (movimiento lateral), humano, exfiltración de datos y simulación WAF y SOC. Los ataques totalmente automatizados y diversificados permiten una prueba de seguridad en cualquier momento, proporcionando a las organizaciones una mejor comprensión de su nivel de seguridad y permitiéndoles mejorarla continuamente.

VAYA UN PASO POR DELANTE DE LOS HACKERS

Los ataques informáticos actuales son más sofisticados y dinámicos que nunca ya que los ciberdelincuentes trabajan constantemente para vulnerar redes, robar propiedad intelectual e interrumpir operaciones. Las organizaciones de todo el mundo invirtieron más de 80 billones de dólares el año pasado para proteger sus datos, bloquear malware y proteger los procesos empresariales críticos.

Aun así, a pesar de todo el tiempo, dinero y esfuerzo invertido en soluciones de ciberseguridad, muchos CISOs aún no pueden responder una pregunta esencial: ¿Cómo de seguros están ahora? Cymulate proporciona la respuesta a esta pregunta con una plataforma de simulación única que permite a las organizaciones validar sus defensas cibernéticas de manera automática y continua.

Ataque por Correo Electrónico

¿POR QUÉ CYMULATE?

Cymulate fue fundada por un equipo de elite de ex oficiales de inteligencia de la IDF, frustrados por las ineficacias de tiempo y recursos que experimentaron mientras realizaban operaciones de seguridad cibernéticas ofensivas en el campo.

Combinando su experiencia en tecnología de simulación cibernética con una amplia experiencia en el campo para imitar los ciberataques más recientes y sofisticados, Cymulate utiliza aplicaciones SaaS de alta gama para simular la gran cantidad de tácticas y estrategias empleadas por los hackers para atacar infraestructuras de seguridad de red.

¿POR QUÉ AHORA?

Las organizaciones suelen relajarse en una falsa sensación de seguridad tras instalar soluciones de seguridad y potenciar su infraestructura.

Cymulate mide de manera real como está preparada la empresa para gestionar amenazas de seguridad informática de forma efectiva.

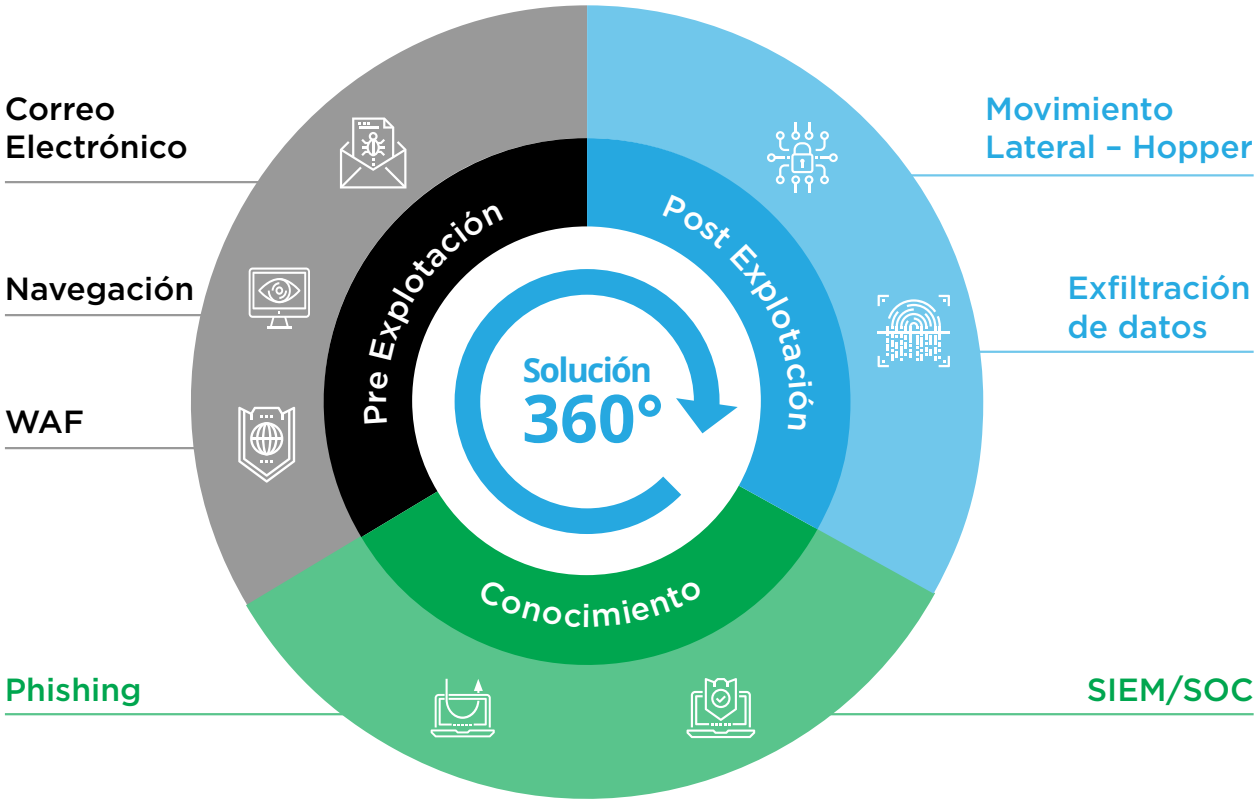
Utilizando acciones ofensivas y defensivas, Cymulate expone las vulnerabilidades críticas simulando ciberataques de múltiples vectores desde la perspectiva del atacante, antes de que un atacante real tenga la posibilidad de explotar cualquier vulnerabilidad.

Las pruebas de Cymulate son sencillas de realizar, en cualquier momento y desde cualquier sitio. Para mantenerse actualizados, recomendamos una prueba mensual.

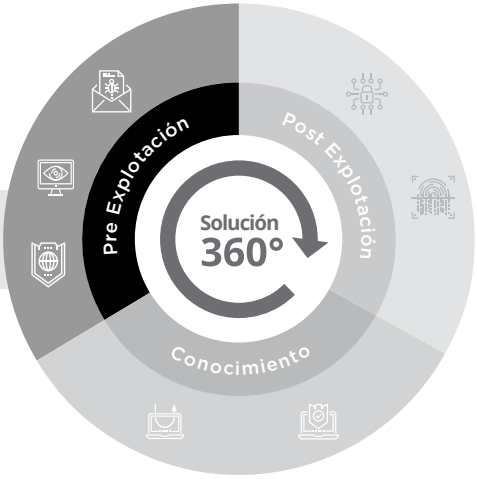
Mientras que la mayoría de las soluciones de ciberseguridad son notoriamente difíciles de implementar, la plataforma Plug & Play de Cymulate es muy fácil, incluso para los usuarios no técnicos.

SOLUCIONES DE CYMULATE

La plataforma de Cymulate se ha dividido en diferentes vectores de ataque proporcionando una visión 360 grados de su nivel de situación ante la seguridad. Analice su seguridad desde la etapa de pre-explotación hasta la etapa de post-explotación para comprender sus vulnerabilidades y mejorar el conocimiento de los empleados de la organización. A través de esta división, podemos proporcionarle con confianza una imagen clara de sus vulnerabilidades desde el punto en el que puede ser vulnerable y qué podría suceder si fuese atacado.



PRE EXPLOTACIÓN



EVALUACIÓN DE CORREO ELECTRÓNICO

Pruebe toda su infraestructura de seguridad de correo electrónico usando nuestros amplios y diversos ataques de correo electrónico

La solución Cymulate Mail permite a las organizaciones desafiar este vector de ataque principal.
La solución Cymulate Mail permite a las organizaciones desafiar este vector de ataque principal. niveEl número de ataques específicamente dirigidos ha aumentado dramáticamente en los últimos años. Una configuración deficiente o la incorrecta implementación de productos de seguridad puede llevar a asumir falsamente que uno está seguro. Esta evaluación le permite validar los supuestos, verificar si se equivocaba y mejorar el nivel de correo electrónico con cada uso.

EVALUACIÓN DE NAVEGACIÓN

Pruebe su exposición de salida HTTP/HTTPS a sitios web maliciosos.

La solución Browsing de Cymulate le permite probar sus capacidades de salida a sitios web maliciosos usando protocolos HTTP/HTTPS comunes. Las pruebas de seguridad de navegación se realizan contra una gran base de datos de sitios web maliciosas que está en continuo crecimiento. La gran mayoría de encuentros con malware en la web se produce mediante la navegación legítima hacia sitios web comunes, incluyendo una gran parte de malware que se entrega a través de complementos del navegador.

EVALUACIÓN DEL FIREWALL DE LA APLICACIÓN WEB

Pruebe su nivel de seguridad WAF en contra de cargas web y proteja mejor sus aplicaciones web

Las aplicaciones web se han convertido en un componente empresarial central en muchas organizaciones, y se gastan enormes cantidades de dinero y esfuerzo en proteger estos activos. Mientras en el pasado los equipos de seguridad TI tenían solo un puñado de aplicaciones web corporativas que defender, ahora necesitan proteger el backend de muchas aplicaciones móviles, aplicaciones SaaS y otras soluciones en la nube. La evaluación WAF está aquí para probar su configuración, implementación y funciones, asegurando que bloquea cargas comunes de aplicación web antes de que se acerquen a sus aplicaciones web.

POST EXPLOTACIÓN

HOPPER - MOVIMIENTO LATERAL

Pruebe su configuración de red de dominio de Windows usando un algoritmo sofisticado

El movimiento lateral dentro de la red en el dominio de Windows es un escenario de penetración común. A medida que los responsables de la amenaza profundizan en la red, sus movimientos y métodos son más difíciles de detectar, especialmente cuando utilizan las funciones de Windows y las herramientas normalmente usadas por los administradores de TI. El sofisticado y eficiente algoritmo del Hopper de Cymulate recopila todas las técnicas comunes y dedicadas que son utilizadas para moverse dentro de la red para revelar los puntos vulnerables de su red en el dominio de Windows.

EVALUACIÓN DE EXFILTRACIÓN DE DATOS

Pruebe sus datos críticos salientes de forma segura antes de exponer los datos reales

Cada vez son más las leyes aprobadas que le imponen a las empresas mayor responsabilidad para salvaguardar sus datos de la mejor manera. Las vulneraciones de datos también tienen un impacto financiero enorme sobre la reputación de la empresa. Las organizaciones dependen de productos para la prevención de pérdida de datos y asegurarse de que nadie puede extraer información crítica fuera de la empresa. Esta evaluación le permite probar su flujo saliente para validar que sus activos principales permanecen dentro.

CONOCIMIENTO

PHISHING Y CONOCIMIENTO

Pruebe la concienciación de sus empleados ante las campañas de phishing

iseñado para reducir el riesgo de “spear-phishing”, ransomware o fraude de CEO, el Phishing de Cymulate puede minimizar el tiempo de desconexión relacionado con el malware, y ahorrar dinero en la reacción a incidentes. Centrados en elevar la concienciación de los empleados sobre la seguridad de la organización mediante la creación y ejecución de campañas de phishing simuladas, buscando enlaces débiles en su organización, y ayudando a crear programas de formación personalizados que mejoran y refuerzan el comportamiento de sus empleados.

EVALUACIÓN DE SIMULACIÓN SIEM/SOC

Pruebe su configuración de alertas SIEM/SOC y el conocimiento de su equipo.

Los equipos SOC normalmente actúan bajo demanda, y a veces se encuentran oxidados. Para adaptar la ciber defensa al panorama de amenazas actual se necesita un enfoque de seguridad proactivo. En vez de reaccionar al último ataque, las organizaciones deben monitorizar continuamente sus redes, cazar atacantes y crear inteligencia estratégica. Esta simulación le permite a las organizaciones probar la correlación de los eventos SIEM y las alertas que el SIEM produce. Además, le permite al CISO probar los procedimientos de Respuesta del equipo SOC ante incidentes.

BENEFICIOS CLAVE

BENEFICIOS CLAVE

Mitigue ataques antes de que sucedan

Cero Falso Positivo

Pruebe toda su seguridad de manera remota

Pruebe sus productos de seguridad - Maximice su ROI

Solución Plug & Play - Fácil de usar

Solución SaaS. No se requiere hardware

Resultados inmediatos: 24/7, 365 días al año

Totalmente automatizado - Pruebas y mejoras continuas

UNIDAD DE INVESTIGACIÓN DE CYMULATE

Con los mejores ingenieros de ingeniería inversa, penetration testers y programadores, la destacada Unidad de soporte cibernético de Cymulate es lo que nos diferencia.

Nuestra función principal es descubrir los puntos débiles en una variedad de vectores y buscar continuamente nuevas vulnerabilidades y fallos.

Con experiencias diversas que abarcan la seguridad privada, experiencia militar y de inteligencia, combinadas con el conocimiento de cómo funciona su negocio, nuestros expertos en seguridad proporcionarán la visibilidad de las amenazas y los responsables de las mismas para que pueda mantener su organización protegida.

Monitorizamos el panorama de amenazas cibernéticas para proporcionar una visión global de las amenazas emergentes, vulnerabilidades de día cero, y las tácticas, técnicas y procedimientos (TTP) de los responsables de amenazas avanzadas. Nuestros investigadores identifican de forma proactiva los métodos de ataques nuevos y únicos mediante la emulación de las tácticas y estrategias de un hacker.

Panel de resultados

ACERCA DE CYMULATE

Cymulate ayuda a las empresas a estar un paso por delante de los ciberdelincuentes con una plataforma de simulación de vulnerabilidades y ataques informáticos que fortalece a las organizaciones con soluciones de seguridad complejas para salvaguardar sus activos críticos de negocio. Al imitar la gama de estrategias que los hackers implementan, el sistema permite a las empresas evaluar su verdadera preparación para gestionar amenazas cibernéticas a la seguridad de forma efectiva. Una plataforma bajo demanda basada en SaaS permite a los usuarios ejecutar simulaciones 24/7 desde cualquier parte, acortando el ciclo de pruebas usual, y acelerando el tiempo hasta la corrección de la situación. Cymulate fue creada en 2016 por ex oficiales de inteligencia de las Fuerzas de Defensa de Israel e investigadores cibernéticos líderes, con una amplia experiencia en soluciones cibernéticas ofensivas.

Para obtener más información, visite **www.cymulate.com**