RESUMEN DE LA SOLUCIÓN

Optimizar la resiliencia ante amenazas

La seguridad proactiva genera resiliencia frente a las amenazas

El riesgo cibernético es un riesgo empresarial. Más del 80% de los consejos de administración consideran la ciberseguridad como una cuestión estratégica para la empresa, por lo que los responsables de seguridad reconocen que su misión es desarrollar la resiliencia necesaria para resistir el próximo ataque.

Más allá de la suposición de brechas y la dependencia excesiva en la detección y respuesta, los líderes en seguridad reconocen tanto la necesidad como la oportunidad de adoptar un enfoque más proactivo en materia de seguridad que adapte continuamente las defensas a las próximas amenazas.

Esta es la esencia de la resiliencia ante las amenazas.

Evidencie la amenaza, mejore la resiliencia

Al probar continuamente sus defensas contra las últimas amenazas avanzadas y toda la cadena de técnicas de ataque, la plataforma de gestión de la exposición de Cymulate proporciona la validación continua, la automatización y la información necesarias para:

- Demostrar su resiliencia ante los ciberataques más avanzados
- Optimizar las contramedidas de seguridad para mejorar la resiliencia frente a amenazas
- Acelerar la ingeniería de detección
- Mida y establezca una postura de referencia en materia de seguridad

La plataforma de gestión de la exposición de Cymulate automatiza la Breach and Attack Simulation (BAS) para la producción, con el fin de realizar pruebas ofensivas que validan continuamente las contramedidas de seguridad mediante las últimas tácticas de amenaza y técnicas de ataque del mundo real.

Validación de amenazas para contramedidas de seguridad esenciales

- Endpoint Security
- Email Gateway
- Detección SIEM
- Protección de cargas de trabajo en la nube
- Detección y respuesta en la nube
- WAF (firewall de aplicaciones web)
- Web Gateway
- Firewall/IPS
- DLP (Prevención de fuga de datos)

Los resultados de estas evaluaciones resaltan las brechas y los puntos débiles de sus defensas de seguridad y le proporcionan orientaciones de corrección para afinar y optimizar sus controles. Como solución SaaS diseñada para implementaciones sencillas y rápidas, Cymulate permite a las organizaciones reforzar sus ciberdefensas, reducir su exposición a las amenazas cibernéticas y demostrar su estado de ciberresiliencia.

Validar la resiliencia ante las amenazas actuales

Con una alimentación diaria de nuevas amenazas activas, la plataforma de gestión de la exposición de Cymulate automatiza la Breach and Attack Simulation (BAS) de las últimas amenazas inmediatas para probar el estado de su resiliencia. El laboratorio de investigación de Cymulate supervisa diariamente la comunidad de inteligencia sobre amenazas para actualizar la plataforma de Cymulate. Las nuevas alertas de amenazas suelen cargarse como simulaciones de amenazas inmediatas en las 24 horas siguientes a la publicación de la alerta.

Beneficios

30% ↑ en prevención de amenazas

Mejora la prevención de amenazas al mitigar las exposiciones probadas y optimizar las contramedidas de seguridad.

3x ↑ en detección de amenazas

Cree, pruebe y ajuste nuevas detecciones de amenazas en cuestión de horas, no semanas.

Pruebe nuevas amenazas en <1 hora

Automatice la validación continua de amenazas con actualizaciones diarias de nuevos ataques y campañas.

Cymulate se integra con nuestro XDR para mejorar nuestra detección y respuesta ante amenazas. Cymulate carga automáticamente los datos críticos sobre amenazas directamente en nuestro XDR para garantizar que las amenazas potenciales se identifiquen y se aborden rápidamente, sin intervención manual.

- Gerente sénior de seguridad, Banco de Singapur

RESUMEN DE LA SOLUCIÓN

Optimizar la resiliencia ante amenazas

La seguridad proactiva genera resiliencia frente a las amenazas

El riesgo cibernético es un riesgo empresarial. Más del 80% de los consejos de administración consideran la ciberseguridad como una cuestión estratégica para la empresa, por lo que los responsables de seguridad reconocen que su misión es desarrollar la resiliencia necesaria para resistir el próximo ataque.

Más allá de la suposición de brechas y la dependencia excesiva en la detección y respuesta, los líderes en seguridad reconocen tanto la necesidad como la oportunidad de adoptar un enfoque más proactivo en materia de seguridad que adapte continuamente las defensas a las próximas amenazas.

Esta es la esencia de la resiliencia ante las amenazas.

Evidencie la amenaza, mejore la resiliencia

Al probar continuamente sus defensas contra las últimas amenazas avanzadas y toda la cadena de técnicas de ataque, la plataforma de gestión de la exposición de Cymulate proporciona la validación continua, la automatización y la información necesarias para:

- Demostrar su resiliencia ante los ciberataques más avanzados
- Optimizar las contramedidas de seguridad para mejorar la resiliencia frente a amenazas
- Acelerar la ingeniería de detección
- Mida y establezca una postura de referencia en materia de seguridad

La plataforma de gestión de la exposición de Cymulate automatiza la Breach and Attack Simulation (BAS) para la producción, con el fin de realizar pruebas ofensivas que validan continuamente las contramedidas de seguridad mediante las últimas tácticas de amenaza y técnicas de ataque del mundo real.

Validación de amenazas para contramedidas de seguridad esenciales

- Endpoint Security
- Email Gateway
- Detección SIEM
- Protección de cargas de trabajo en la nube
- Detección y respuesta en la nube
- WAF (firewall de aplicaciones web)
- Web Gateway
- Firewall/IPS
- DLP (Prevención de fuga de datos)

Los resultados de estas evaluaciones resaltan las brechas y los puntos débiles de sus defensas de seguridad y le proporcionan orientaciones de corrección para afinar y optimizar sus controles. Como solución SaaS diseñada para implementaciones sencillas y rápidas, Cymulate permite a las organizaciones reforzar sus ciberdefensas, reducir su exposición a las amenazas cibernéticas y demostrar su estado de ciberresiliencia.

Validar la resiliencia ante las amenazas actuales

Con una alimentación diaria de nuevas amenazas activas, la plataforma de gestión de la exposición de Cymulate automatiza la Breach and Attack Simulation (BAS) de las últimas amenazas inmediatas para probar el estado de su resiliencia. El laboratorio de investigación de Cymulate supervisa diariamente la comunidad de inteligencia sobre amenazas para actualizar la plataforma de Cymulate. Las nuevas alertas de amenazas suelen cargarse como simulaciones de amenazas inmediatas en las 24 horas siguientes a la publicación de la alerta.

Beneficios

30% ↑ en prevención de amenazas

Mejora la prevención de amenazas al mitigar las exposiciones probadas y optimizar las contramedidas de seguridad.

3x ↑ en detección de amenazas

Cree, pruebe y ajuste nuevas detecciones de amenazas en cuestión de horas, no semanas.

Pruebe nuevas amenazas en <1 hora

Automatice la validación continua de amenazas con actualizaciones diarias de nuevos ataques y campañas.

Cymulate se integra con nuestro XDR para mejorar nuestra detección y respuesta ante amenazas. Cymulate carga automáticamente los datos críticos sobre amenazas directamente en nuestro XDR para garantizar que las amenazas potenciales se identifiquen y se aborden rápidamente, sin intervención manual.

- Gerente sénior de seguridad, Banco de Singapur

Postura de seguridad de referencia e identificación de desviaciones

Con pruebas automatizadas continuas, Cymulate crea una base de referencia de la postura en materia de seguridad, detecta disminuciones inesperadas en la cobertura de amenazas y proporciona pruebas del estado actual de la resiliencia cibernética. Las características principales incluyen:

- Dashboards de seguridad y mapas de riesgo MITRE ATT&CK que señalan los puntos fuertes, los puntos débiles y los niveles de exposición
- Los informes técnicos y ejecutivos proporcionan pruebas y evidencia de la postura de seguridad con tendencias de desempeño
- Análisis de desviaciones que identifica los cambios en las configuraciones de las contramedidas de seguridad y en el entorno que afectan a la postura de seguridad
- Estudio comparativo de mercado (Benchmarking) del sector para contrastar la eficacia de la seguridad con la de sus homólogos

Optimizar la prevención y detección de amenazas

Cymulate proporciona soluciones prácticas y automatizadas para la corrección y mitigación de riesgos. Cymulate se integra con las contramedidas de seguridad para movilizar acciones con detección recomendada y mitigación automatizada a fin de bloquear amenazas activas.

Pase de la exposición a la mitigación con la prevención inmediata

Cuando Cymulate identifica una amenaza que no se ha podido prevenir, la plataforma incluye la opción de enviar actualizaciones para esa amenaza específica directamente al control de seguridad para su prevención inmediata. Al combinar la validación y la mitigación, la plataforma de Cymulate proporciona a los equipos de seguridad la tecnología y las integraciones necesarias para automatizar las tareas manuales y optimizar la resiliencia ante amenazas.

Crear reglas de detección personalizadas

Basándose en los resultados de las pruebas y las deficiencias en la cobertura de amenazas, Cymulate proporciona reglas de detección personalizadas. Dependiendo de la amenaza y el control de seguridad, estas reglas de detección de Cymulate siguen estándares del sector como Sigma o incluyen traductores de consultas para asignar las reglas recomendadas al formato específico del proveedor para SIEM, EDR y XDR.

Asignar reglas SIEM a la biblioteca de ataques con IA

Cymulate se integra con SIEM para validar las reglas de detección existentes al implementar la IA a fin de comparar escenarios de ataque relevantes con cada regla de detección. Cymulate comprueba si las reglas se activan según lo previsto, descubre fallos de detección y recibe recomendaciones específicas para mejorar la lógica de las reglas. Con la automatización integrada, Cymulate facilita la comprobación y el ajuste continuos de las reglas, lo que garantiza una protección duradera contra las amenazas en constante evolución en la full kill-chain.

> **Mediante las integraciones de Cymulate, lanzamos evaluaciones para comprobar si nuestras herramientas las detectan. Si no es así, Cymulate proporciona orientación sobre medidas de mitigación y reglas Sigma, y volvemos a ejecutar fácilmente las evaluaciones para validar la corrección.**
>
> - Karl Ward, Responsable de ciberseguridad, LV=

¿Por qué elegir Cymulate?

Validación continua de amenazas

La mejor validación de exposición de su clase con una única plataforma para optimizar los controles, ampliar las pruebas ofensivas y proporcionar información esencial sobre la exposición.

Automatización sencilla

Pruebas avanzadas para cualquier miembro del Blue Team o Red Team que se pueden ejecutar y personalizar con plantillas, mejores prácticas y asistente de IA para escalar las pruebas ofensivas.

Ponga la “T” en CTEM

Convierta la validación de amenazas en un proceso continuo con la colaboración entre los equipos de operaciones de seguridad, inteligencia sobre amenazas y VM (gestión de vulnerabilidades).

Postura de seguridad de referencia e identificación de desviaciones

Con pruebas automatizadas continuas, Cymulate crea una base de referencia de la postura en materia de seguridad, detecta disminuciones inesperadas en la cobertura de amenazas y proporciona pruebas del estado actual de la resiliencia cibernética. Las características principales incluyen:

- Dashboards de seguridad y mapas de riesgo MITRE ATT&CK que señalan los puntos fuertes, los puntos débiles y los niveles de exposición
- Los informes técnicos y ejecutivos proporcionan pruebas y evidencia de la postura de seguridad con tendencias de desempeño
- Análisis de desviaciones que identifica los cambios en las configuraciones de las contramedidas de seguridad y en el entorno que afectan a la postura de seguridad
- Evaluación comparativa del sector para contrastar la eficacia de la seguridad con la de sus homólogos

Optimizar la prevención y detección de amenazas

Cymulate proporciona soluciones prácticas y automatizadas para la corrección y mitigación de riesgos. Cymulate se integra con las contramedidas de seguridad para movilizar acciones con detección recomendada y mitigación automatizada a fin de bloquear amenazas activas.

Pase de la exposición a la mitigación con la prevención inmediata

Cuando Cymulate identifica una amenaza que no se ha podido prevenir, la plataforma incluye la opción de enviar actualizaciones para esa amenaza específica directamente al control de seguridad para su prevención inmediata. Al combinar la validación y la mitigación, la plataforma de Cymulate proporciona a los equipos de seguridad la tecnología y las integraciones necesarias para automatizar las tareas manuales y optimizar la resiliencia ante amenazas.

Crear reglas de detección personalizadas

Basándose en los resultados de las pruebas y las deficiencias en la cobertura de amenazas, Cymulate proporciona reglas de detección personalizadas. Dependiendo de la amenaza y el control de seguridad, estas reglas de detección de Cymulate siguen estándares del sector como Sigma o incluyen traductores de consultas para asignar las reglas recomendadas al formato específico del proveedor para SIEM, EDR y XDR.

Asignar reglas SIEM a la biblioteca de ataques con IA

Cymulate se integra con SIEM para validar las reglas de detección existentes al implementar la IA a fin de comparar escenarios de ataque relevantes con cada regla de detección. Cymulate comprueba si las reglas se activan según lo previsto, descubre fallos de detección y recibe recomendaciones específicas para mejorar la lógica de las reglas. Con la automatización integrada, Cymulate facilita la comprobación y el ajuste continuos de las reglas, lo que garantiza una protección duradera contra las amenazas en constante evolución en la full kill-chain.

> **Mediante las integraciones de Cymulate, lanzamos evaluaciones para comprobar si nuestras herramientas las detectan. Si no es así, Cymulate proporciona orientación sobre medidas de mitigación y reglas Sigma, y volvemos a ejecutar fácilmente las evaluaciones para validar la corrección.**
>
> - Karl Ward, Responsable de ciberseguridad, LV=

¿Por qué elegir Cymulate?

Validación continua de amenazas

La mejor validación de exposición de su clase con una única plataforma para optimizar los controles, ampliar las pruebas ofensivas y proporcionar información esencial sobre la exposición.

Automatización Automatización

Pruebas avanzadas para cualquier miembro del Blue Team o Red Team que se pueden ejecutar y personalizar con plantillas, mejores prácticas y asistente de IA para escalar las pruebas ofensivas.

Ponga la “T” en CTEM

Convierta la validación de amenazas en un proceso continuo con la colaboración entre los equipos de operaciones de seguridad, inteligencia sobre amenazas y VM (gestión de vulnerabilidades).