Nuestra **única prioridad** es la ciberseguridad de nuestros clientes

ICE
ISRAEL
CYBERSECURITY
ENTERPRISE

# Guía paso a paso para implementar una estrategia de Red Team ganadora

CYE

www.ice.lat

# Introducción

Los equipos rojos (Red Teams) actualmente son noticia, pero muchas organizaciones tienen dudas sobre qué hacen exactamente y cómo pueden trabajar con sus propios grupos de seguridad. Esta guía explica qué es un equipo rojo, por qué es necesario, cómo opera, cómo trabajar con equipos externos e internos, y mucho más. Un equipo rojo es un grupo de personas altamente calificadas que emulan los métodos de ataque que utilizaría un atacante real. A veces llamados "hackers éticos", ellos ayudan a mejorar la ciberseguridad de las organizaciones revelando deficiencias en las defensas de ciberseguridad y cómo podría explotarlas un atacante real. El objetivo de un ejercicio de 'Red Teaming' (simulación de un ataque en la vida real), según el NIST[1], es "mejorar la ciberseguridad de la empresa demostrando los impactos de ataques exitosos".

El equipo rojo puede proporcionar confianza a la dirección en su postura de seguridad gracias a los resultados obtenidos en el contexto del panorama actual de las ciber amenazas. El equipo rojo generalmente trabaja en conjunto con un equipo azul (Blue Team) interno -los defensores- quienes son responsables de mantener la postura de seguridad de la organización.

El equipo rojo lleva a cabo tareas de reconocimiento, se infiltra en las redes e intenta acceder a activos empresariales valiosos, proporcionando deducciones relevantes para que el equipo azul pueda ayudar a la organización a estar preparada para el próximo ataque. El equipo rojo es astuto, pues imita el enfoque de los hackers sofisticados, pero al mismo tiempo debe seguir siendo ético y profesional. Esto requiere de un equipo experimentado y profesional que conozca a fondo las tácticas, técnicas y procedimientos (TTP) de los atacantes, así como las herramientas y marcos que utilizan.

Los ejercicios de los equipos rojos generalmente tienen lugar una o dos veces al año. Sin embargo, cuando se produce un ataque importante, tiene sentido realizar una evaluación por parte del equipo rojo que se centre en ese ataque específico (por ejemplo, un ataque de 'ransomware' [ciber secuestro de datos] que afecte a otras organizaciones del mismo sector).

Esto puede revelar deficiencias que la organización debe atender si quiere responder adecuadamente. Muchas organizaciones tienen su propio equipo rojo interno, el cual lleva a cabo ejercicios periódicos de ‘Red Teaming’. Aun así, la mayoría de las empresas querrán mejorarlo con equipos externos. Los equipos internos pueden verse indebidamente influenciados por la organización y la política de la compañía, o pueden concentrarse en métodos específicos excluyendo otros que podrían suponer una amenaza mayor. El mejor modo de proceder es utilizar equipos rojos tanto internos como externos[3]. Esto ofrece flexibilidad para incorporar nuevas perspectivas y hacer frente rápidamente a las amenazas emergentes, teniendo en cuenta que se tarda una media de 277 días[4] para descubrir y contener una brecha.

# Pasos para una estrategia eficaz del equipo rojo

La intervención de un equipo rojo no es una tarea rápida. Implica varios pasos y algunos de ellos pueden ser largos. Éstos incluyen:

1) Determinar el alcance de la intervención
2) Recopilar información general
3) Investigación y reconocimiento
4) Desarrollar el plan de trabajo
5) Ejecutar el plan, descubriendo debilidades y deficiencias que no se han detectado
6) Documentar y comunicar los hallazgos

## Paso 1. Determinar el alcance de la intervención

El primer paso consiste en llevar a cabo debates entre la organización objetivo y el equipo rojo con el propósito de llegar a un acuerdo sobre el alcance de la intervención, los objetivos finales y, sobre todo, las reglas de intervención. ¿Se atacará toda la infraestructura de TI o sólo partes específicas? ¿Puede establecer el equipo rojo un centro de mando y control? ¿Están prohibidas determinadas tácticas?

Los debates preliminares permitirán al equipo comprender plenamente qué objetivos específicos están dentro del alcance y qué tipos de ataque están permitidos, como los ataques a aplicaciones web, los intentos de penetración en la red y los ataques de ingeniería social, como el 'spear phishing' ('phishing' focalizado).

Un aspecto clave de la fase de preparación es asegurarse de que tanto el equipo rojo como la organización objetivo comprendan perfectamente el cronograma de la intervención. Dado que una intervención típica puede durar entre 4 y 5 meses, es importante establecer las expectativas desde el principio. El equipo rojo no informará al cliente de cuándo se llevará a cabo el ciberataque, ni el equipo interno de defensa sabrá que se está planeando una intervención del equipo rojo. Sin embargo, la organización debe asegurarse de que se están agrupando los registros pertinentes y de que se han configurado las alertas como parte del programa normal de defensa de la seguridad. Además, es muy importante definir un punto de contacto en la organización y un canal de comunicación, con el fin de diferenciar las alertas generadas por las actividades del equipo rojo y una amenaza real.

Recomendación: El equipo rojo debe obtener una carta de autorización del cliente o de la dirección de la organización concediéndole permiso para realizar ciberataques.

## Paso 2. Recopilar información general

El segundo paso consiste en explorar a fondo la organización. Es entonces cuando el equipo aprende lo más posible sobre los empleados, la tecnología y las defensas de seguridad de la organización objetivo. Este esfuerzo implica recopilar información detallada sobre qué aplicaciones

se ejecutan, qué sitios se utilizan, qué servicios son fundamentales para la organización y sobre los propios empleados. La información sobre los empleados es especialmente importante cuando se trata de los que trabajan en los equipos de seguridad y del SOC (centro de operaciones de seguridad): conocer su ubicación física, horario normal de trabajo, especialidades y cualquier información personal que pueda obtenerse de las redes sociales y otras fuentes abiertas forma parte del perfil general de la organización objetivo. Cuando se trata de una organización con varias sedes, el equipo rojo recopila información específica de cada región, determinando las horas de trabajo específicas, los días festivos y las costumbres que podrían afectar a las operaciones, y revela las horas libres óptimas en las que un ataque del equipo rojo sería más difícil de detectar.

## Paso 3. Investigación y reconocimiento

Esta es la fase que permite al equipo rojo recopilar información detallada sobre los objetivos de la intervención. La información incluida en esta fase puede incluir:

- Redes y operaciones: se incluyen los rangos de direcciones IP, así como cualquier puerto de red abierto, terminales API para dispositivos móviles y controles de seguridad establecidos. El equipo busca posibles puntos de infiltración y exfiltración (fuga de información).

- Información sobre los empleados: se identifica a las personas objetivo y se recopila información detallada sobre cada empleado de la organización. La información valiosa incluye direcciones de correo electrónico, perfiles en redes sociales, números de teléfono, departamentos y cargos, números de identificación y similares. El equipo rojo encuentra objetivos de alto valor, como los empleados que trabajan en los equipos de seguridad o SOC, así como aquellos que probablemente tengan privilegios elevados. El equipo también intenta identificar a los empleados que pueden ser víctimas de ataques de ingeniería social, como el personal no técnico.

- Vulnerabilidades: esta actividad implica centrarse en las vulnerabilidades más recientes, ya que es muy probable que la organización objetivo aún no las haya "parchado". El equipo incluirá vulnerabilidades específicas en el plan de trabajo eventual, y desarrollará métodos de ataque y explotación hechos a medida para cada una de ellas.

## Paso 4. Desarrollar el plan de trabajo

Cuando se ha recopilado toda la información anterior, el equipo rojo crea su plan de trabajo centrándose en los métodos de ataque, fechas, horas y objetivos. El equipo creará ataques de ingeniería social específicos para la organización objetivo, además de desarrollar cargas maliciosas y personas falsas según sea necesario. Todos los métodos utilizados

por el equipo rojo deben emular las TTP de los atacantes reales.

Evidentemente, esta planeación y preparación exige un sofisticado trabajo de ingeniería; el equipo tendrá que desarrollar sus propios métodos para explotar vulnerabilidades nuevas o emergentes. Los equipos rojos expertos construirán un

laboratorio que duplique el entorno exacto de la empresa objetivo. En el laboratorio, el equipo investiga a fondo cada vulnerabilidad que será explotada y crea sus propios métodos para aprovecharla. A continuación, cada método se prueba minuciosamente antes de ejecutarlo, para asegurarse de que no activará una alerta. Todo esto es complejo y lleva mucho tiempo, pero el resultado final será un mayor índice de éxito. Los ataques de ingeniería social son una herramienta clave en el arsenal del equipo rojo. Basándose en la información recopilada durante la fase de investigación y reconocimiento, el equipo será capaz de determinar qué tipos de ataque podrían dirigirse a aquellos empleados que tienen más probabilidades de ser víctimas.

## Ingeniería social y métodos de ataque de contraseña

Bombardeo de solicitudes de MFA: la autenticación multifactor es una herramienta valiosa para impedir la usurpación de cuentas, ya que requiere que el usuario proporcione un factor adicional además del nombre de usuario y la contraseña. Sin embargo, las versiones más antiguas de MFA que emplean contraseñas de una única vez o solicitudes automáticas pueden utilizarse para engañar a los usuarios enviando múltiples solicitudes de MFA al dispositivo, hasta que el usuario finalmente cede y acepta la autenticación. Ataques de 'spear phishing': ataques específicos por correo electrónico que parecen proceder de un remitente de confianza, a menudo utilizando información extraída de fuentes abiertas, como publicaciones en redes sociales. El objetivo es infectar el dispositivo del usuario con 'malware' (programa maligno) o conseguir que revele información, como sus credenciales. Compromiso del correo electrónico empresarial (BEC): el correo electrónico parece proceder de una empresa o persona de confianza, como el director general, el departamento de recursos humanos o el de finanzas de la organización. En lugar de ser legítimo, contiene un enlace de 'phishing', un archivo adjunto malicioso u otro método para acceder a la red.

Recomendaciones: Asegúrese de que el equipo rojo dispone de un laboratorio sofisticado capaz de duplicar el entorno exacto del objetivo y de personalizar la explotación de las vulnerabilidades emergentes.
Asegúrese de elegir un equipo rojo con experiencia en la creación de ataques de ingeniería social hechos a la medida, y que no se limite simplemente a utilizar métodos de ataque comunes que probablemente sean detectados. Esto podría incluir ataques de fuerza bruta, ataques de pulverización de contraseñas o correos electrónicos de 'phishing' ampliamente disponibles.

## Paso 5. Ejecutar el plan

El equipo rojo basará su cronograma en las mejores fechas y horarios para intentar acceder a cada una de las regiones relevantes. Al ejecutar el plan según este cronograma, el equipo intenta irrumpir en la red mediante un ataque a una vulnerabilidad no "parchada", ataques personalizados de ingeniería social u otro método hecho a la medida para evadir la

detección. Una vez que el equipo ha obtenido acceso a la red, trabaja de forma encubierta, ganando terreno y logrando persistencia. Todo este tiempo, el equipo se hace pasar por usuarios normales para no provocar una alarma. El equipo

rojo establecerá un centro de comando y control (C2) para poder comunicarse con el exterior sin ser detectado dentro de la red. Mientras está dentro, el equipo recopila información y realiza más reconocimientos, moviéndose lateralmente por toda la red. Al hacerlo, encuentra oportunidades para escalar privilegios y realizar otras acciones diseñadas para alcanzar el objetivo de apoderarse del dominio (en entornos AD [directorio activo]). Cuando eso ocurra, el equipo rojo tendrá acceso a todas las computadoras y usuarios de la organización. Si se hubiera tratado de un atacante real, los daños podrían haber sido graves, incluyendo el bloqueo de todo el equipo de seguridad. Cuando el equipo rojo se apodera del dominio, suele considerarse una victoria.

Recomendaciones: Asegúrese de que el equipo rojo tiene la capacidad de establecer su propio C2 con el fin de permanecer sigiloso mientras recopila información y de que no recurra a productos estándar que sean fáciles de detectar. Si el equipo del SOC recibe una alerta, y el POC (punto de contacto) verifica que se debe a la actividad del equipo rojo, permita que el equipo proceda como lo haría normalmente. Solo intervenga si se va a producir una interrupción del negocio - por ejemplo, una 'reimaging' (reinstalación de la imagen del sistema) que podría dejar fuera de servicio a servidores clave durante horas o días.

### Paso 6. Documentar los hallazgos

Durante la fase de ejecución, el equipo rojo documenta todas las acciones llevadas a cabo y los resultados producidos. El último paso de la intervención del equipo rojo es reportar las acciones, reacciones y resultados a las partes relevantes, incluyendo la gerencia de TI, el CSO (director de seguridad), el CISO (director de seguridad de la información), el CIO (director de información) y otros, según corresponda. El reporte debe documentar clara y completamente lo que funcionó y lo que no. Debe incluir detalles sobre las vulnerabilidades descubiertas y cómo podría explotarlas un atacante real. El reporte también debe incluir recomendaciones para acciones futuras. Puede destacar las mejores prácticas de corrección, así como los planes de mitigación más rentables con base en las necesidades específicas de la organización.
Recomendaciones: El reporte también debe incluir recomendaciones para acciones futuras. Puede destacar las mejores prácticas de corrección, así como los planes de mitigación más rentables con base en las necesidades específicas de la organización.

## ¿Cómo elegir un equipo rojo?

Los CISO que consideran una estrategia de equipo rojo como parte de su plan de seguridad a menudo se enfrentan a la elección de crear un equipo interno o contratar a un tercero. La contratación de un equipo externo es casi siempre un buen enfoque, tenga o no la organización un equipo interno, ya que proporciona flexibilidad, imparcialidad y un equipo amplio y experimentado. De hecho, dada la escasez

de "red teamers" (miembros de equipo rojo) calificados en el mercado, puede resultar difícil construir un equipo interno robusto. Por lo tanto, recurrir a proveedores externos puede ser sensato para casi cualquier organización.

Seleccionar a un proveedor de equipos rojos implica asegurarse de que éste cuenta con las aptitudes tácticas, técnicas y estratégicas requeridas, incluyendo un profundo conocimiento y comprensión de los sistemas, protocolos, herramientas y medidas de seguridad.

**Las capacidades clave incluyen:**

- Un sólido historial de éxito en intervenciones de equipos rojos en organizaciones similares.
- Capacidad demostrada para actuar de manera ética y profesional.
- Sólidas aptitudes de ingeniería social: capacidad para crear ataques personalizados de ingeniería social a la medida de la organización objetivo.
- Un sofisticado laboratorio que pueda duplicar el entorno de la organización objetivo.
- Sólidas aptitudes de desarrollo de ciberseguridad, incluyendo la capacidad de personalizar la explotación de las vulnerabilidades emergentes.
- Habilidad para crear una capacidad encubierta de mando y control
- Excelentes aptitudes de comunicación con todos los niveles de la organización

## ¿Cómo puede ayudar CYE?

Hyver, la plataforma de optimización de ciberseguridad de CYE, permite a las empresas evaluar, cuantificar y mitigar los ciber riesgos para que puedan tomar mejores decisiones en materia de seguridad e invertir en correcciones eficaces.

CYE combina la tecnología con la actividad de los equipos rojos para brindar las evaluaciones de seguridad organizativa más completas, así como el análisis contextual y deducciones relevantes sobre los riesgos.

CYE proporciona una completa visibilidad de las posibles rutas de ataque; agiliza y establece prioridades en el proceso de corrección, y permite a los responsables de seguridad comprender mejor el costo real de las amenazas y la corrección.

Utilizando CYE, las compañías pueden eliminar la necesidad de numerosas herramientas de ciberseguridad y reducir la probabilidad y el impacto de los ciberataques.


+52 (55) 1710 8373 | info@ice.lat | www.ice.lat
CDMX, México