METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #20 DETECCIÓN DE EQUIPO ROJO

Pautas para detectar y responder a actividades del Equipo Rojo.

Autor IRM: CERT SG
Contribución: CERT a Dvens / Paloma Vargas
Versión del IRM: 2.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

Traducción al Español

Paloma Amilene Vargas Alvarado
E-Mail: amilenhalvarado@gmail.com
Twitter / X: @AmileneVargas

CONTENIDO

1. ABSTRACTO

Esta metodología de respuesta a incidentes es una guía rápida dedicada a los encargados para detectar e investigar problemas de seguridad relacionados con ejercicios del equipo rojo dentro de la organización.

¿QUIÉN DEBE UTILIZAR HOJAS IRM?

- Administradores.
- Centro de Operaciones de Seguridad.
- CISO y adjuntos.
- CERT (Equipo de respuesta ante emergencias informáticas).

Recuerde: Si crees que has detectado un ejercicio del Equipo Rojo, sigue el IRM, toma notas y contacta inmediatamente al equipo de Respuesta a Incidentes de tu línea de negocio, CERT u otro equipo Azul aplicable si es necesario

Objetivo de IRM: El objetivo de la Metodología de Respuesta a Incidentes para la Detección de Equipo Rojo (IRM20) es ofrecer un enfoque bien estructurado y sistemático para identificar, gestionar y abordar incidentes que involucren las acciones de un Equipo Rojo o de cualquier otra entidad de seguridad ofensiva que tenga como objetivo los sistemas de información de una organización. Intrínsecamente, esta metodología busca mejorar las capacidades generales de la organización para detectar, investigar y mitigar posibles amenazas cibernéticas perpetradas por actores de amenazas avanzadas.

2. PASOS PARA LA GESTIÓN DE INCIDENTES

SE DEFINEN 6 PASOS PARA GESTIONAR INCIDENTES DE SEGURIDAD

1. **Preparación**: prepárese para manejar el incidente
2. **Identificación**: detectar el incidente
3. **Contención**: limitar el impacto del incidente
4. **Remediación**: eliminar la amenaza
5. **Recuperación**: recuperarse a una etapa normal
6. **Lecciones aprendidas**: elaborar y mejorar el proceso

IRM proporciona información detallada para cada paso del proceso de respuesta a incidentes. Los pasos provienen de la Guía de Gestión de Incidentes de Seguridad Informática del NIST.

2.1 PREPARACIÓN

OBJETIVO: ESTABLECER CONTACTOS, DEFINIR PROCEDIMIENTOS, REUNIR INFORMACIÓN PARA AHORRAR TIEMPO DURANTE UN INCIDENTE REALIZADO POR UN EQUIPO ROJO.

- Desarrollar canales de comunicación para informar a las partes interesadas sobre los ejercicios detectados del Equipo Rojo; hay que tener en cuenta la posible existencia de membresías solapadas en los equipos Azul y Blanco para evitar conflictos de intereses.
- Identificar a los posibles miembros existentes del equipo blanco y establecer puntos de contacto con ellos.
- Utilizar sistemas de detección de intrusiones basados en red y en el host. Asegúrate de que estén configurados correctamente para monitorizar eficazmente el tráfico de red y los sistemas de endpoint en busca de actividades maliciosas. Asegúrate de que el registro y monitorización seguros de las actividades de red y sistema esté establecido, que los eventos se registren correctamente, se transmitan a SIEM y que existan reglas aplicables y probadas para imponer alertas.
- Configura y prueba regularmente las herramientas SIEM a tu disposición para recopilar, analizar y reaccionar a eventos de seguridad. Estas herramientas pueden calibrarse para detectar indicios de actividades del Red Team, como fallos de inicio de sesión, cambios de configuración e intentos de reconocimiento de red.
- Asegúrate de que tus soluciones actuales de protección de endpoints proporcionen controles adecuados contra malware mediante detección estática y dinámica. Asegúrate de que todos los tipos de endpoints y servidores estén cubiertos, incluyendo diferentes sistemas operativos de escritorio y servidor, dispositivos móviles y BYODs (si procede).
- Definir puntos de contacto específicos las 24 horas del día y las personas que intervengan en caso de emergencia.
- Establecer puentes operativos bien funcionales entre los equipos Blue existentes (SOC, CERT, otros contrapartes de seguridad); realiza regularmente ejercicios conjuntos de respuesta a incidentes incorporando miembros de diferentes equipos Azules.
- Revisa y evalúa regularmente los controles, políticas y procedimientos de seguridad de tu organización.
- Implementar un control procedimental llamado "Botón Rojo" para detener o suspender temporalmente todas las actividades de redteaming en caso de necesidad operativa (coincidiendo con incidentes reales, impacto en la producción, etc.).
- Preparar estrategias, procedimientos y herramientas de comunicación internas y externas para usar durante un incidente del Equipo Rojo, incluyendo canales alternativos para excluir fugas de información entre los miembros del equipo Azul y Rojo.

- Proporcionar al personal del equipo Azul un conocimiento actualizado sobre las amenazas cibernéticas, el papel del equipo Rojo y los métodos que puedan utilizar. Esto incluye patrones de ataque previos, TTPs comúnmente empleados y IOCs ya vistos. Proporcionar acceso a informes de misión previamente realizados por el Equipo Rojo y a las lecciones aprendidas si se considera posible.
- Asegúrese de preparar la documentación formal de la misión, incluyendo todos los documentos aplicables como las Reglas de Enfrentamiento, los Objetivos de la Misión, la Descripción Detallada del Escenario, la tarjeta de Salida de la Cárcel y cualquier documentación adicional de patrocinio de partes interesadas clave, como CISO, CTO, etc.

Prepárate para notificar a los altos directivos si es necesario durante un incidente de Equipo Rojo.

2.2 IDENTIFICACIÓN

OBJETIVO: DETECTAR EL INCIDENTE, DETERMINAR SU ALCANCE E INVOLUCRAR A LAS PARTES APROPIADAS.

Es posible que necesite notificar a los interesados, socios y reguladores al inicio de este paso si es necesario.

Detección.

- Monitoree signos de compromiso y comportamiento inusual en su entorno (movimiento lateral, mecanismos de persistencia, etc.).
- Investigue alertas de seguridad y analice registros en busca de indicadores de posible actividad del Red Team.
- Haga la triage de incidentes potenciales para determinar si pueden ser parte de un ejercicio del Red Team.
- Evalúe la magnitud y las posibles consecuencias de la actividad identificada del Red Team. Consulte con el equipo White en caso de duda para evitar manejar incorrectamente un incidente generado por un actor de amenaza real.
- Una vez validado el incidente, determine qué sistemas están afectados, qué datos pueden haber sido expuestos o exfiltrados y cuál es el impacto potencial general que este incidente puede generar en las operaciones del negocio. Proporcionar respuestas adecuadas puede requerir imaginar los objetivos finales perseguidos por el Red Team.
- Involucre a todos los interesados previamente identificados, incluyendo pero no limitándose a los equipos Blue, áreas de negocio, soporte de infraestructura y personal general de seguridad de la información; evalúe el impacto potencial con base en la información disponible sobre el incidente y en los comentarios recibidos de los colegas de negocio y TI.
- Evalúe posibles escenarios de remediación, como bloquear interconexiones, reforzar el monitoreo con base en la evaluación de riesgo frente a los posibles impactos en la producción. Sea extremadamente cauteloso para no revelar a los miembros del Red Team que han podido ser identificados.
- Si la validación y el alcance confirman un incidente conocido del Red Team, escálelo a la alta dirección. Proporcióneles todos los detalles necesarios de manera exacta y oportuna.
- Haga que los coordinadores del equipo White establezcan canales de comunicación con los interesados correspondientes para compartir información continuamente sobre el ejercicio en curso. Si la naturaleza del incidente lo requiere, configure canales alternativos dedicados (no corporativos) para usar en la comunicación e intercambio de datos durante el ejercicio.

Considera consultar otros IRM que puedan ser aplicables a la misión sospechosa del Red Team:

- **IRM-2-Detección de Intrusiones en Windows**
- **IRM-3-Detección de Intrusiones en Unix/Linux**
- **IRM-7-Detección de Malware en Windows**
- **IRM-10-Ingeniería Social**
- **IRM-11-Fuga de Información**
- **IRM-14-Estafa**
- **IRM-16-Phishing**
- **IRM-17-Ransomware**
- **IRM-18-Compromiso a Gran Escala**

2.3 CONTENCIÓN

OBJETIVO: PREVENIR EL DESARROLLO DE NUEVOS ATAQUES Y LIMITAR SU ALCANCE.

- Aísle todas las máquinas comprometidas o sistemas afectados para prevenir intrusiones adicionales o la propagación del ataque.
- Implemente controles de acceso y segmentación de la red para limitar el alcance del ataque.
- Organice reuniones regulares con el proveedor afectado, incorporando a los interesados correspondientes.
- Coordínese con los interesados empresariales afectados para implementar medidas de contención, como aislar sistemas comprometidos, bloquear IOCs maliciosos o cambiar credenciales, de acuerdo con los requisitos de seguridad del negocio.
- Simule contramedidas riesgosas o potencialmente impactantes para evitar pérdidas en producción.

Si el tráfico crítico para el negocio no puede desconectarse, permítalo después de implementar controles de seguridad adicionales para detectar e inhibir oportunamente la propagación lateral.

Si es aplicable a los IOC 'Rojos' identificados (verifique dos veces antes de aplicarlos, ya que podrían desencadenar reacciones nefastas por parte del equipo rojo):

- Bloquee el tráfico hacia los C2 identificados.
- Bloquee el acceso hacia/desde cualquier elemento de infraestructura roja aplicable.
- Desactive o restrinja las cuentas comprometidas por los atacantes.
- Envíe muestras no detectadas a su proveedor de seguridad de endpoints, proveedores de AV y plataformas sandbox.
- Envíe URL maliciosas, nombres de dominio e IP no categorizadas a sus proveedores de seguridad.

Puede considerar simular contramedidas arriesgadas o potencialmente impactantes para evitar efectos indeseables del ejercicio en producción.

2.4 REMEDIACIÓN

OBJETIVO: ELIMINAR LOS ACCESOS DEL EQUIPO ROJO Y ASEGURAR SUS SISTEMAS.

- Revisar de manera exhaustiva los hallazgos de las fases anteriores. Determinar los puntos de acceso iniciales del equipo Rojo, las posiciones en los sistemas, las actividades laterales y los mecanismos de persistencia para asegurarse de que estén completamente identificados.
- Asegurarse de que las vulnerabilidades explotadas por el equipo Rojo y otros métodos de ataque aplicables estén bien comprendidos.
- Una vez que todas las tácticas, métodos y vulnerabilidades estén identificadas, priorízalas según su impacto potencial en la seguridad. Comienza a aplicar parches en las vulnerabilidades de mayor riesgo, descendiendo hacia las menos críticas.
- Basándose en los hallazgos, fortalece la configuración de los sistemas para prevenir futuras explotaciones. Esto puede implicar medidas como ajustar la configuración de seguridad, limitar los privilegios de los usuarios, deshabilitar servicios innecesarios y refinar las reglas del firewall. Esto también es aplicable a la fase de lecciones aprendidas.
- Localiza y elimina cualquier mecanismo de persistencia, puerta trasera o webshell que el equipo Rojo pueda haber dejado en tus sistemas durante el ejercicio. Realiza una investigación exhaustiva para asegurarte de que no queden vulnerabilidades derivadas ni caminos de acceso ocultos.
- Realiza pruebas de validación para confirmar que las acciones de remediación han asegurado eficazmente los sistemas comprometidos. Verifica que el equipo Rojo o cualquier otra entidad ofensiva no pueda volver a explotar las vulnerabilidades previamente identificadas.
- Documenta debidamente todos los pasos de remediación, sus resultados y cualquier desafío encontrado durante el proceso. Transmite resúmenes de las correcciones y soluciones a los interesados relevantes, incluyendo las descripciones de cómo estas vulnerabilidades fueron explotadas por el equipo Rojo. Este paso también se aplica a la fase de Lecciones Aprendidas.

Recomendaciones adicionales de diligencia: en caso de signos de lateralización, consulte el IRM 18 – Compromiso a Gran Escala.

2.5 RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A SUS OPERACIONES NORMALES.

Todos los pasos siguientes deben realizarse de manera gradual y con supervisión técnica de los equipos Azul, Rojo, Blanco o Púrpura.

- Confirma la efectividad de las estrategias de remediación utilizadas. Verifica que las vulnerabilidades hayan sido parcheadas, que las configuraciones del sistema estén reforzadas y que los mecanismos de persistencia hayan sido eliminados. Los sistemas deben estar seguros antes de restaurar las operaciones normales.
- Restaura los sistemas y servicios a su estado operativo normal. En algunos casos, esto puede implicar pasos adicionales, como reconstruir o remasterizar los sistemas, restaurar datos desde copias de seguridad o migrar a plataformas completamente nuevas, dependiendo del alcance del ataque del Red Team.
- Una vez que los sistemas se hayan restaurado de manera efectiva, realiza pruebas funcionales y de seguridad exhaustivas para garantizar que tus sistemas funcionen de manera óptima y no sean vulnerables a tipos similares de actividades del Red Team en el futuro. Trabaja con los propietarios de los negocios afectados para restaurar todos los servicios o sistemas impactados, asegurando que estén seguros y libres de vulnerabilidades.
- Monitorea el rendimiento de tus sistemas para detectar cualquier anomalía o problema de seguridad como parte de la fase de Recuperación. Asegúrate de que los sistemas estén operando normalmente y hayan mantenido sus niveles de rendimiento previos al ejercicio del Red Team.
- Declara el fin de la fase de recuperación solo cuando hayas confirmado que tus sistemas han vuelto a la normalidad, son seguros y estables. Cualquier anomalía o impacto del ejercicio del Red Team debe haber sido completamente abordado.

2.6 LECCIONES APRENDIDAS

OBJETIVO: DOCUMENTAR LOS DETALLES DEL INCIDENTE, DISCUTIR LAS LECCIONES APRENDIDAS Y AJUSTAR LOS PLANES Y LAS DEFENSAS.

Informe

Un informe de misión del Equipo Rojo debe ser redactado y puesto a disposición de todas las partes interesadas involucradas. Pueden requerirse diferentes formatos del informe para presentarlos a distintas audiencias en diferentes niveles estratégicos, operativos y tácticos.

Se deberán describir los siguientes temas:

- Causa inicial de la infección
- Acciones y cronogramas de cada evento importante
- ¿Qué salió bien?
- ¿Qué salió mal?
- Costo del incidente
- Indicadores de compromiso

Capitalizar

- Documente los hallazgos del ejercicio, incluyendo métodos de ataque, vulnerabilidades e impactos; este conocimiento verificado puede ayudar en futuras misiones de respuesta a incidentes.
- Evalúe la efectividad de los controles de detección y respuesta.
- Identifique áreas de mejora e implemente cambios en los procesos y defensas.
- Comparta el conocimiento obtenido del ejercicio con los interesados relevantes.
- Realice una reunión de análisis con todas las partes involucradas. El Equipo Rojo debería presentar su metodología, tácticas, técnicas y procedimientos, y explicar cómo aprovecharon las vulnerabilidades del sistema.
- Realice un análisis detallado de toda la operación de respuesta a incidentes, desde la detección hasta la recuperación. Identifique lo que funcionó bien, lo que no, y dónde existen oportunidades de mejora.
- Documente los conocimientos adquiridos del ejercicio, detallando los desafíos enfrentados y sus soluciones. Compile una lista de elementos que requieran acciones de remediación adicionales, especificando quién debe ser responsable de implementar estos cambios.
- Basándose en las lecciones aprendidas, desarrolle un plan de acción integral para abordar las brechas identificadas. Priorice las actividades según su importancia y urgencia para asegurarse de que los riesgos más altos se traten de manera inmediata (victorias rápidas).

- Dedique una persona para dar seguimiento al avance de estas implementaciones. Esta acción podría ser asignada al Equipo Púrpura.
- Comuníquese los hallazgos y las lecciones aprendidas a un espectro más amplio de interesados. Esto podría extenderse a toda la organización para mejorar la conciencia y el comportamiento de seguridad en general.
- Planifique una auditoría de seguimiento a mediano y largo plazo para verificar la implementación efectiva de los elementos del plan de acción derivados de los hallazgos de la misión del Equipo Rojo.

Un ejercicio del equipo rojo puede considerarse como una fase previa para un proyecto de mejora continua como Equipo Morado.

3. DEFINICIONES

CONCEPTO	DESCRIPCIÓN
IRM	Metodología de Respuesta a Incidentes
CISO	Chief Information Security Officer (ejecutivo responsable de la seguridad de la información)
CERT	Equipo de Respuesta a Incidentes Informáticos
NIST	Instituto Nacional de Estándares y Tecnología
Red Team	Entidades de seguridad ofensiva que simulan ataques reales contra los sistemas de la organización para probar las defensas.
Blue Team	Personal de defensa (SOC, CERT) encargado de detectar, investigar y mitigar las amenazas.
White Team	Miembros que actúan como árbitros o coordinadores del ejercicio, con quienes se debe validar si un incidente es una simulación o un atacante real.
Purple Team	Un enfoque de mejora continua donde se integran conocimientos de ataque y defensa; pueden encargarse de dar seguimiento al plan de acción post-ejercicio.
TTPs (Tactics, Techniques, and Procedures)	Patrones de ataque, métodos y técnicas comúnmente empleados por actores de amenazas avanzados.
Rules of Engagement (Reglas de Compromiso):	Documentación formal que define los límites, objetivos y alcances del ejercicio de Red Team.
Getting-out-of-Jail Card	Documento de autorización que certifica que las actividades sospechosas detectadas son parte de un ejercicio autorizado.
Reconocimiento de Red	Intentos de los atacantes por mapear la infraestructura y sistemas activos.
Mecanismos de Persistencia	Métodos (como backdoors o webshells) que el Red Team deja en los sistemas para mantener el acceso a largo plazo.
Red Button (Botón Rojo)	Control procedimental para detener inmediatamente todas las actividades del Red Team en caso de necesidad operativa o impacto real en producción.
Infraestructura Roja	Elementos técnicos (servidores, dominios) utilizados por el equipo ofensivo para ejecutar el ataque.

C2 (Command and Control)	Centros de comando identificados desde los cuales se controla la intrusión; el IRM sugiere bloquear el tráfico hacia ellos una vez detectados.
Endurecimiento (Harden system configurations)	Refuerzo de las configuraciones de seguridad, como limitar privilegios de usuario y desactivar servicios innecesarios, para prevenir futuras explotaciones.
Triaje	Proceso de evaluación inicial para determinar si una alerta de seguridad es un ejercicio de Red Team o una amenaza real.
Lateralización (Lateral Movement)	Movimientos del atacante a través de la red después del compromiso inicial; el documento refiere al IRM 18 para este escenario.
Remasterización de Sistemas	Acción de reconstruir sistemas desde cero o desde copias de seguridad seguras durante la fase de recuperación.