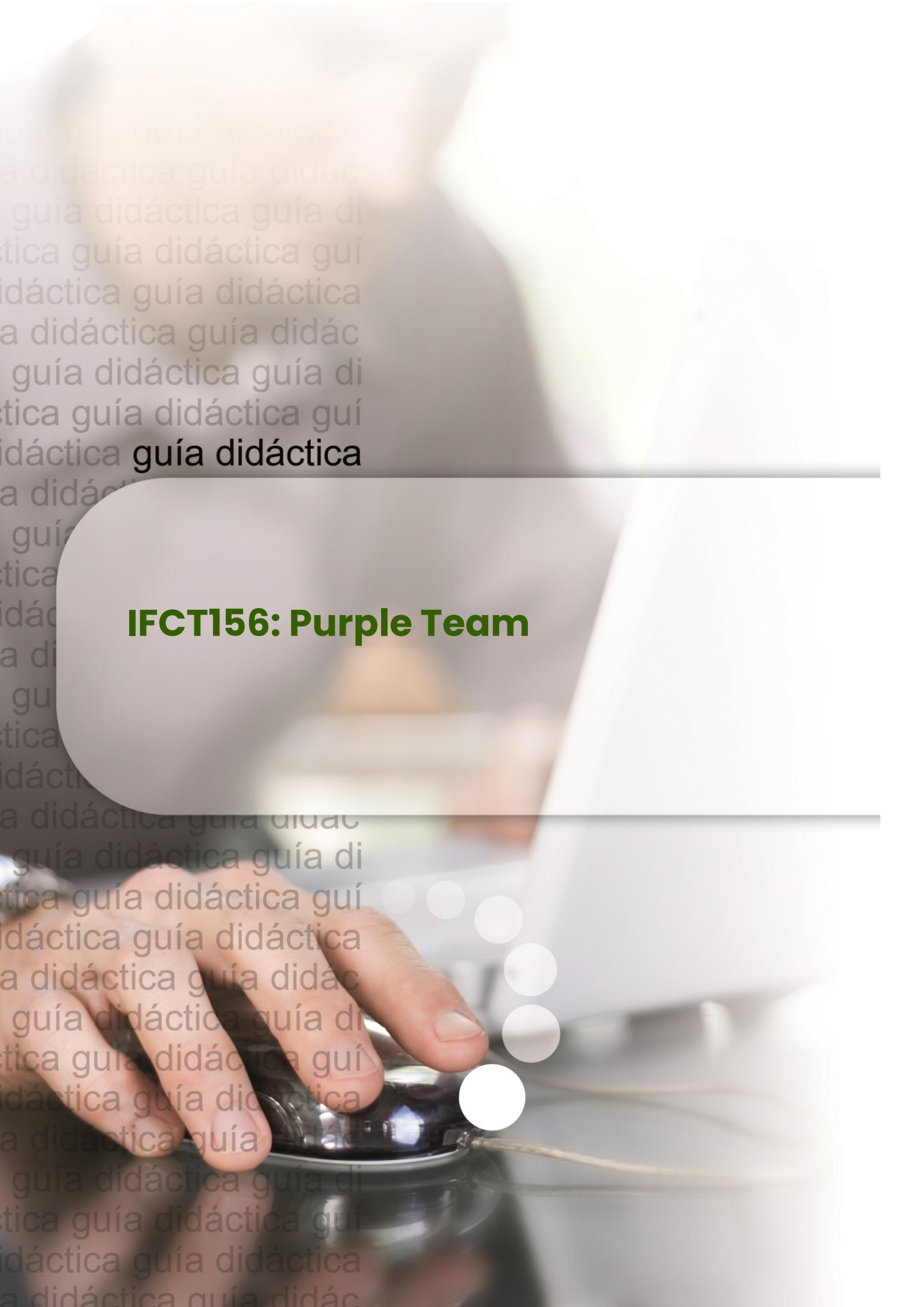

IFCT156: Purple Team

Objetivo general

- Integrar las tácticas y controles defensivos del Blue Team con las amenazas y vulnerabilidades encontradas por el Red Team.

Objetivos específicos

- Planificar pruebas de seguridad mediante objetivos, alcance, reglas de enfrentamiento, ventanas de trabajo y criterios de finalización.
- Definir los elementos operativos necesarios para preparar entornos, accesos, dependencias, comunicaciones y registro de evidencias.
- Analizar el enfoque Purple Team como modelo colaborativo entre capacidades ofensivas y defensivas orientado a mejorar la detección, la respuesta y la resiliencia.
- Diferenciar las funciones de Red Team, Blue Team y Purple Team, identificando sus responsabilidades, límites y sinergias dentro de un ejercicio de ciberseguridad.
- Analizar amenazas reales para diseñar medidas defensivas alineadas con los activos del negocio.
- Seleccionar fuentes de inteligencia de amenazas atendiendo a criterios de calidad, relevancia y aplicabilidad.
- Traducir TTPs en controles preventivos, detectivos y correctivos vinculados a escenarios de ataque.
- Identificar brechas de visibilidad, cobertura y respuesta mediante el estudio de casos prácticos.
- Analizar la ejecución de una emulación de adversario mediante la comparación entre acciones planificadas, telemetría generada y resultados defensivos observados.
- Diseñar guiones de emulación secuenciados que representen técnicas realistas de acceso, persistencia, escalada, evasión, descubrimiento, movimiento lateral y acciones sobre objetivos.

- Verificar la capacidad de los sistemas defensivos para registrar, correlacionar y alertar sobre comportamientos asociados a una intrusión simulada.
- Medir la eficacia de la respuesta defensiva a partir de detecciones generadas, trazas disponibles, tiempos de detección y tiempos de respuesta.
- Analizar los principios de detección como código aplicados al Purple Team, valorando la gestión de reglas, parseadores, enriquecimientos y documentación.
- Diseñar y ejecutar pruebas automatizadas sobre reglas de detección, definiendo entradas, expectativas y aserciones y generando datos sintéticos y reproducibles.
- Integrar las detecciones en pipelines de CI/CD, gestionando entornos separados y aplicando despliegues controlados con capacidad de rollback.
- Administrar el ciclo de vida del contenido de detección mediante un catálogo de estados, ownership y la gestión de excepciones, supresiones y reglas temporales.
- Comprender la estructura de un informe Purple Team, diferenciando alcance, hipótesis, resultados, narrativa ejecutiva y anexo técnico.
- Definir métricas de desempeño que permitan evaluar detección, cobertura, tiempos operativos y calidad de la respuesta.
- Interpretar evidencias, línea temporal e indicadores observados para relacionar la actividad emulada con la capacidad defensiva.
- Diseñar un plan de remediación con backlog priorizado, criterios de verificación de cierre y seguimiento de mejoras.

- **Contenidos**

IFCT156. Purple Team	Tiempo estimado
Módulo 1: Purple Team	
Unidad 1: Purple Team y la ciberseguridad. 1. Planificación de pruebas. 1.1. Objetivos de la prueba y preguntas a responder. 1.2. Alcance, exclusiones y criterios de finalización. 1.3. Selección del escenario y nivel de realismo requerido. 1.4. Reglas de enfrentamiento, ventanas de trabajo y condiciones de parada. 1.5. Preparación de entorno, accesos y dependencias. 1.6. Plan de comunicaciones y coordinación operativa. 1.7. Registro de evidencias, trazabilidad y custodia. 2. Definición y principios del Purple Team en el contexto de ciberseguridad. 3. Diferencias y sinergias entre Red Team, Blue Team y Purple Team.	
Cuestionario de Autoevaluación UA 01	**30 minutos**
Actividad de Evaluación UA 01	**45 minutos**
Tiempo total de la unidad	**9 horas**
Unidad 2: Planificar e implementar una defensa de amenazas informada. 1. Definición de medidas. 1.1. Fuentes de inteligencia de amenazas y criterios de calidad. 1.2. Modelado de amenazas orientado al negocio y activos críticos. 1.3. Traducción de TTPs en requisitos de control (preventivos, detectivos y correctivos) 1.4. Ingeniería de detecciones: reglas, correlaciones y umbrales. 1.5. Controles de hardening y reducción de superficie de ataque. 1.6. Gestión de vulnerabilidades y parcheo informados por amenazas.	

2. Análisis de casos prácticos. 2.1. Selección de casos alineados a perfiles de adversario y sector. 2.2. Descomposición del ataque en fases para identificar oportunidades defensivas. 2.3. Identificación de brechas de visibilidad, cobertura y capacidad de respuesta.	
Cuestionario de Autoevaluación UA 02	**30 minutos**
Actividad de Evaluación UA 02	**45 minutos**
Tiempo total de la unidad	**10 horas**
Unidad 3: Realizar la emulación de adversario. 1. Análisis y evaluación de la ejecución. 1.1. Preparación del guion de emulación y secuenciación de acciones. 1.2. Instrumentación y verificación de la telemetría durante la ejecución. 1.3. Ejecución controlada de técnicas y validaciones previas por paso. 1.4. Simulación de acceso inicial y establecimiento de persistencia. 1.5. Simulación de escalada de privilegios y evasión defensiva. 1.6. Simulación de descubrimiento y movimiento lateral. 1.7. Simulación de acciones sobre objetivos: exfiltración, impacto y/o interrupción. 1.8. Medición de resultados: detecciones generadas, trazas y tiempos de respuesta.	
Cuestionario de Autoevaluación UA 03	**30 minutos**
Actividad de Evaluación UA 03	**45 minutos**
Tiempo total de la unidad	**8 horas**
Unidad 4: Detección como código y automatización de pruebas. 1. Principios de detección como código (DaC) aplicados a Purple Team. 1.1. Estructura del repositorio: reglas, parsers, enriquecimientos y documentación asociada. 1.2. Convenciones de nomenclatura, versionado y trazabilidad de cambios. 1.3. Revisión por pares y criterios de aceptación para cambios en contenido de detección.	

2. Diseño de pruebas automatizadas para detecciones. 2.1. Pruebas unitarias de reglas: entradas, expectativas y aserciones. 2.2. Generación de eventos sintéticos y datasets reproducibles para pruebas. 2.3. Reproducción de logs (replay) y simulación controlada de secuencias de actividad. 3. Integración con pipelines y entornos. 3.1. CI/CD para contenido de SIEM/EDR/XDR: empaquetado, test y despliegue. 3.2. Separación de entornos (laboratorio, preproducción, producción) y promoción controlada. 3.3. Rollback y gestión de incidencias derivadas de cambios en detecciones. 4. Gobierno del ciclo de vida del contenido de detección. 4.1. Catálogo de detecciones: estados (borrador, activo, deprecated) y ownership. 4.2. Gestión de excepciones, supresiones y reglas temporales con justificación.	
Cuestionario de Autoevaluación UA 04	**30 minutos**
Actividad de Evaluación UA 04	**45 minutos**
Tiempo total de la unidad	**14 horas**
Unidad 5: Reporte, métricas y cierre del ciclo Purple Team. 1. Estructura del informe Purple Team: alcance, hipótesis y resultados. 1.1. Narrativa ejecutiva orientada a impacto y riesgo. 1.2. Anexo técnico: evidencias, línea temporal e indicadores observados. 2. Definición de métricas de desempeño del ejercicio. 2.1. Métricas de detección y cobertura frente a TTPs emuladas. 2.2. Métricas operativas: tiempos de alerta, triage, contención y recuperación. 3. Plan de remediación y seguimiento de mejoras. 3.1. Priorización del backlog y criterios de verificación de cierre.	
Cuestionario de Autoevaluación UA 05	**30 minutos**
Actividad de Evaluación UA 05	**45 minutos**
Tiempo total de la unidad	**8 horas**
Examen final	**1 hora**
5 unidades	**50 horas**