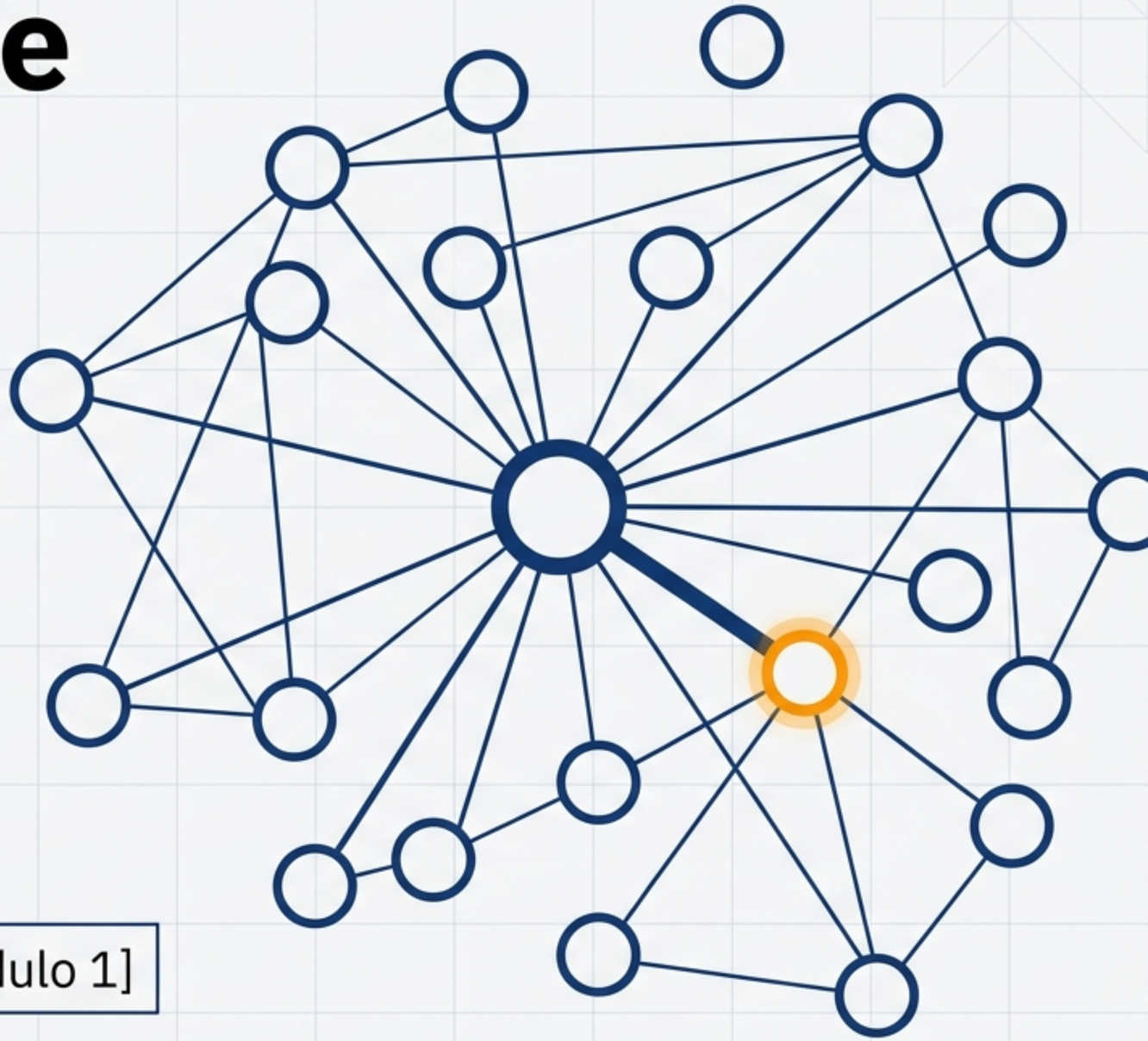
Fundamentos de Ciberseguridad Defensiva

Construyendo la **mentalidad analítica** para entornos SOC



[Curso de Ciberseguridad Defensiva - Módulo 1]

El plan de ruta del analista

Entender la misión

Proteger la continuidad operativa de la empresa, no solo frenar hackers.

Dominar el idioma

Diferenciar con precisión clínica entre amenaza, vulnerabilidad y riesgo.

Pensar como analista

Preparar la base teórica para interpretar telemetría real (Wazuh / T-Pot).

¿Qué es realmente la ciberseguridad?

MITO

Es solo frenar ataques maliciosos.

Es instalar un antivirus.

Es una cuestión puramente tecnológica.

REALIDAD

Es proteger activos digitales y operativos frente a ataques, abusos y fallos.

Es evitar errores humanos y fugas de información.

Es garantizar que el negocio siga funcionando.

EJEMPLO SOC: Un SOC no protege ordenadores en abstracto.
Protege accesos, usuarios y datos críticos para la empresa.

El motor de la defensa: Los 4 pilares

La **Tríada CIA:** Qué estamos protegiendo

Dos enfoques: **Ofensiva** vs. **Defensiva**

Seguridad Ofensiva

Objetivo
Buscar el fallo y evaluar la seguridad.

La Pregunta Clave
¿Cómo puedo entrar o romper este sistema?

Ejemplo
Un pentester descubre una credencial remota débil antes que un atacante real.

Focus

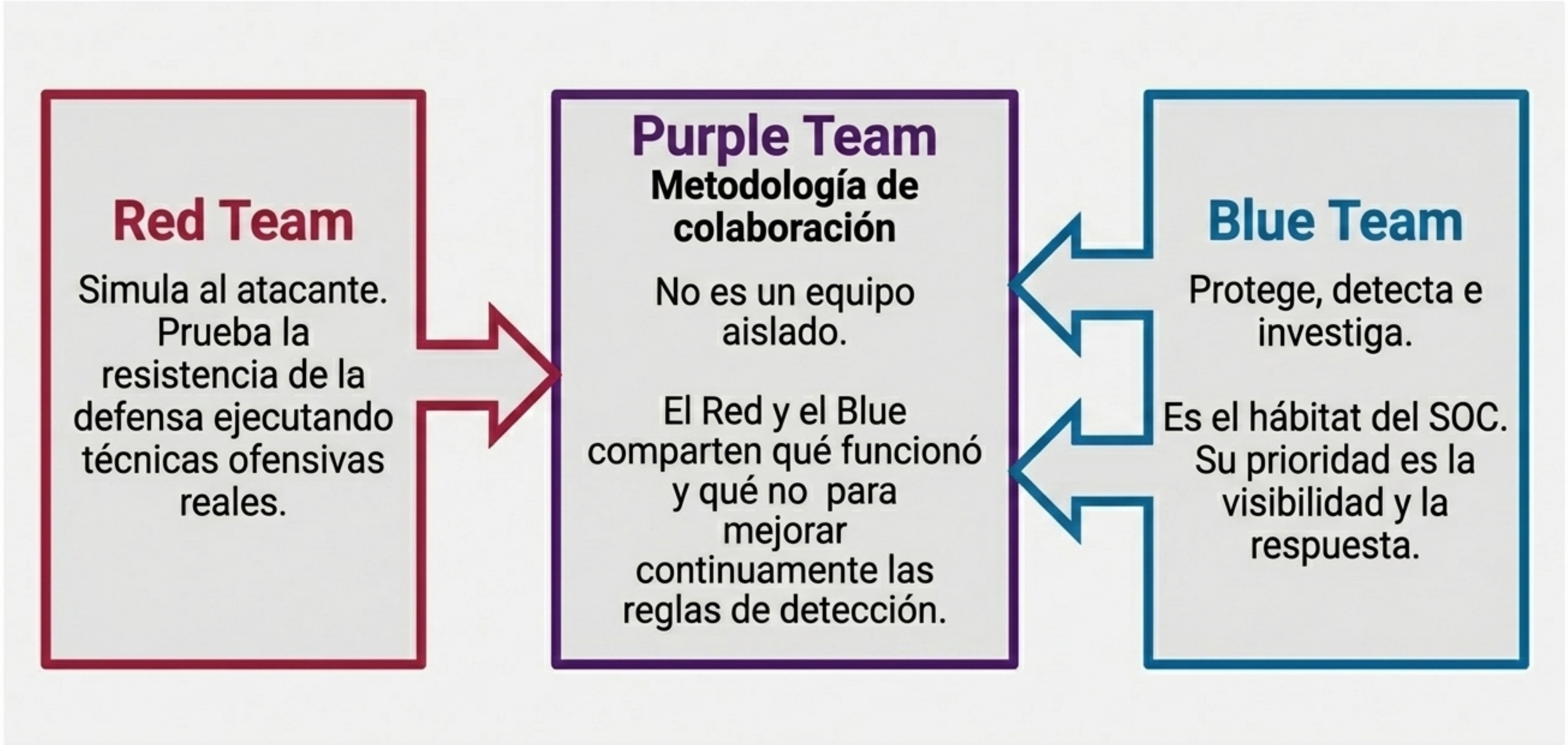
Seguridad Defensiva (Foco del Curso)

Objetivo
Prevenir, monitorizar, investigar y responder.

La Pregunta Clave
¿Cómo veo que alguien está intentando entrar?

Ejemplo
El analista SOC detecta múltiples intentos fallidos, correlaciona la actividad y aísla la amenaza.

El ecosistema operativo: **Red, Blue y Purple Team**



El campo de batalla: ¿Qué protege el analista?

Operaciones Críticas

La capacidad real de la empresa para seguir prestando servicios y hacer negocio.

Identidades y Accesos

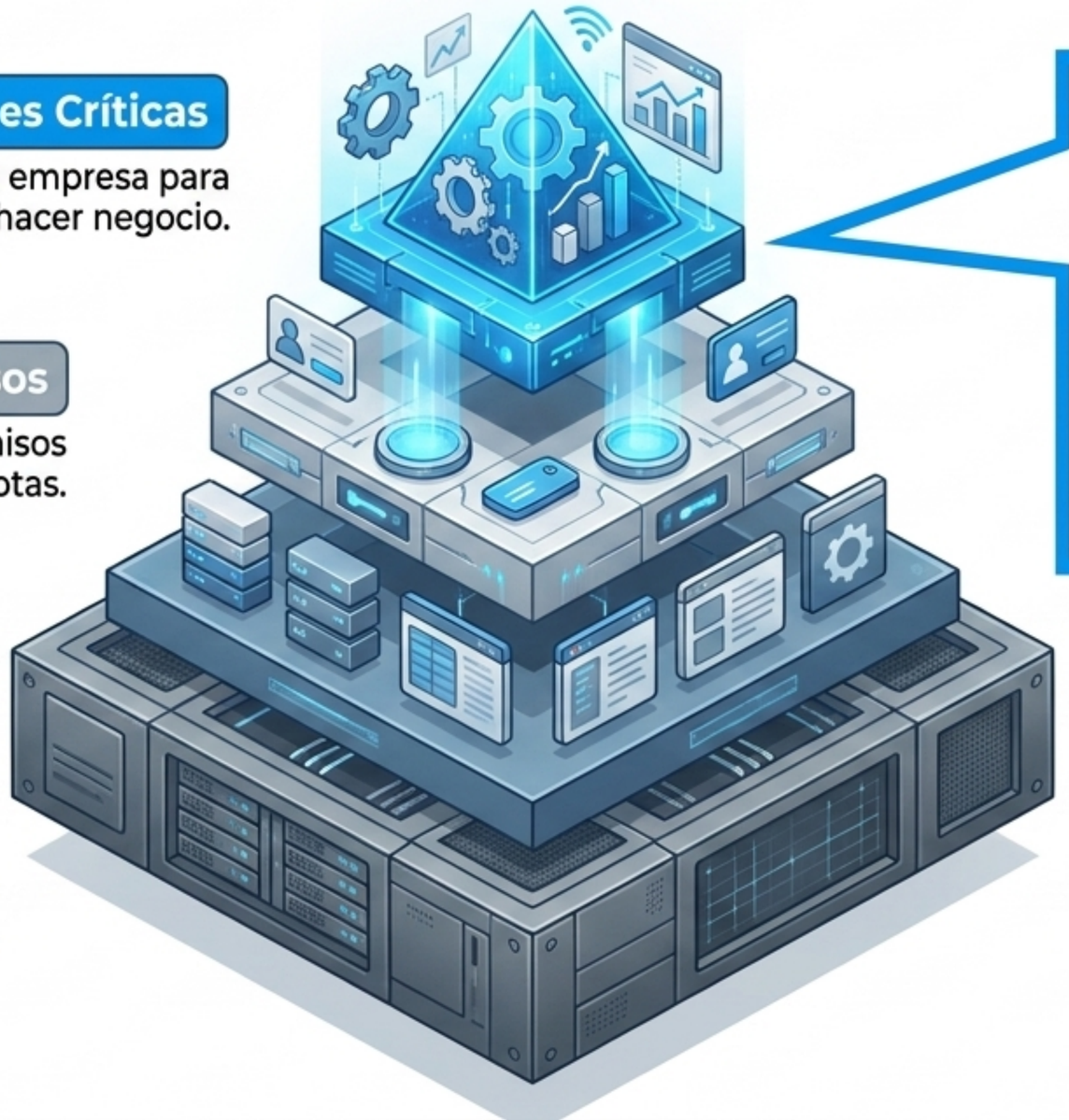
Cuentas de usuario, permisos privilegiados, conexiones remotas.

Datos y Aplicaciones

Bases de datos, código, software de gestión, correos.

Infraestructura

Redes, servidores, equipos físicos.

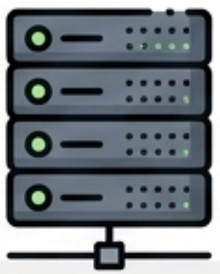


Un analista no protege máquinas de forma aislada; protege identidades, activos y procesos de negocio.

Priorización: Activos y Activos Críticos

Un **Activo** es cualquier elemento con valor. Un **Activo Crítico** es aquel cuya caída paraliza la organización. El contexto del negocio dicta el impacto del evento

Baja Criticidad



Servidor de pruebas de laboratorio aislado

Intento de acceso fallido

Baja urgencia.
Valor formativo / estadístico.

Alta Criticidad

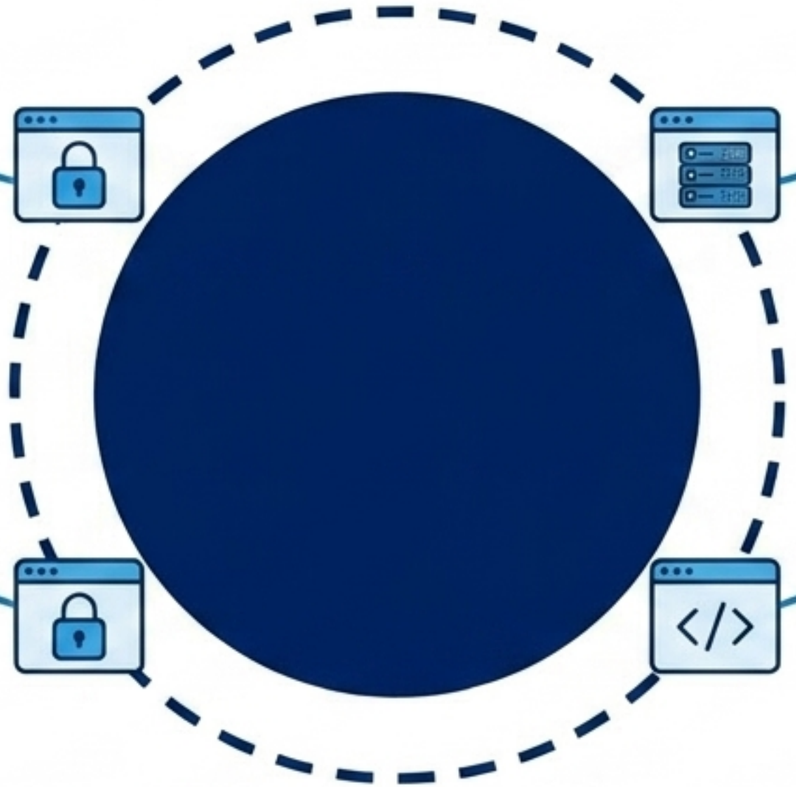
Controlador de Dominio / Cuenta Admin

Intento de acceso idéntico

Severidad máxima.
Escalado e investigación inmediata.

La Superficie de Ataque

El conjunto de puntos por los que un atacante puede interactuar con una organización. Todo punto accesible aumenta el riesgo.



Servicios Expuestos

Puertos abiertos, servidores web (SSH, RDP).

Accesos

VPN corporativa, portales de empleados.

Credenciales

Contraseñas débiles, filtraciones públicas.

Código y Lógica

APIs expuestas, configuraciones inseguras.

La superficie no es solo la red pública; incluye identidades, correos y errores operativos.

Desmontando el Peligro: La Ecuación del Riesgo

Amenaza (Quién / Qué)

Aquello que intenta causar daño.

Ejemplo:
Actor malicioso o un fallo interno grave.

Vulnerabilidad (El Fallo)

La debilidad explotable en el sistema.

Ejemplo:
Servicio expuesto sin parchear o credenciales por defecto.

Impacto (El Daño)

El resultado si la amenaza tiene éxito.

Ejemplo:
Robo de datos, caída del servidor web.

Riesgo (La Consecuencia)

La probabilidad de que ocurra combinada con la gravedad del impacto.

Un puerto abierto no es una vulnerabilidad por sí sola; el riesgo nace al combinarlo con la amenaza y el impacto.

Riesgo = Amenaza x Vulnerabilidad x Impacto

Anatomía de una Intrusión

Paso 1: Actor Malicioso

Concepto:
Quien impulsa la actividad dañina.

Ejemplo:
Un bot automatizado o un atacante humano.

Paso 2: Vector de Ataque

Concepto:
El camino o mecanismo utilizado para interactuar.

Ejemplo:
Un servicio SSH expuesto a Internet.

Paso 3: Explotación

Concepto:
El aprovechamiento de una condición favorable.

Ejemplo:
Uso de un diccionario para adivinar una credencial débil.

Paso 4: Compromiso

Concepto:
Lograr acceso, control o acción sobre el objetivo.

Ejemplo:
Obtener shell interactiva y ejecutar comandos.

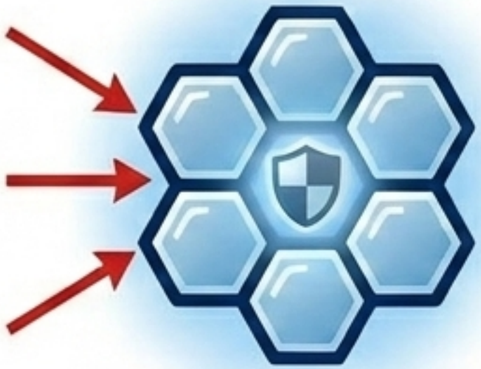
Nota: No todo intento de explotación resulta en compromiso.

Síntesis: De la Teoría al Mini-SOC

El Ataque

Un Actor usa un Vector contra nuestra Superficie de Ataque.

La Trampa (T-Pot)



El honeypot absorbe el impacto. No es un Activo Crítico, pero genera telemetría defensiva.

La Visibilidad (Wazuh)

El SOC recibe el log. El analista evalúa la Amenaza, descarta el Compromiso real, y extrae inteligencia táctica.

El Tablero Completo (Resumen del Módulo)

Amenazas operando sobre la **Superficie de Ataque**

El **Blue Team** **utiliza visibilidad** para **Detectar y Responder**

Con el fin de **mitigar** el **Riesgo** y prevenir el **Compromiso**

Objetivo Final: Proteger los Activos Críticos y mantener la Confidencialidad, Integridad y Disponibilidad (CIA) del negocio.

5 Leyes del Analista SOC (Para Recordar)

1. La ciberseguridad protege operaciones de negocio, no solo ordenadores.
2. Asume que la prevención fallará; la detección y respuesta rápidas salvan a la empresa.
3. Un evento sin contexto de negocio no significa nada. Prioriza por la criticidad del activo.
4. Amenaza, Vulnerabilidad, Impacto y Riesgo son conceptos distintos matemáticamente ligados. Úsalos con precisión.
5. No todo intento es una explotación, y no toda explotación resulta en compromiso. Mide hasta dónde llegó el atacante.