**1. Ejemplos de Acciones Posibles del Atacante**

Un atacante podría intentar diversas acciones para comprometer una plataforma web. Algunos ejemplos comunes son:

* **SQL Injection:** Inyección de código SQL malicioso en formularios web para manipular la base de datos.
* **Cross-Site Scripting (XSS):** Inserción de scripts maliciosos en páginas web para ejecutar código en el navegador de la víctima.
* **Ataques de Fuerza Bruta:** Intentos repetidos de adivinar contraseñas o credenciales.
* **DDoS (Distributed Denial of Service):** Envío masivo de tráfico para saturar la plataforma y hacerla inaccesible.
* **Robo de Sesión:** Interceptación de cookies de sesión para suplantar a usuarios legítimos.
* **Phishing:** Uso de sitios falsos o correos electrónicos engañosos para obtener datos personales.
* **Escaneo de Vulnerabilidades:** Exploración automatizada de la plataforma para identificar puntos débiles en la seguridad.

**2. Funciones del Sistema de Detección de Ataques**

El **sistema de detección** de ciberataques (IDS - *Intrusion Detection System*) tiene varias funciones clave:

1. **Monitoreo en Tiempo Real:** Supervisar constantemente el tráfico y los eventos de la plataforma.
2. **Análisis de Logs:** Revisar los registros de actividad para identificar patrones inusuales.
3. **Detección de Anomalías:** Identificar comportamientos que no se alinean con la actividad normal del usuario.
4. **Reglas de Firma:** Comparar eventos con una base de datos de patrones conocidos de ataques (como firmas de ataques SQL o XSS).
5. **Alertas y Notificaciones:** Enviar alertas automáticas a los administradores cuando se detecte un posible ataque.
6. **Mitigación de Amenazas:** Aplicar bloqueos o restricciones (por ejemplo, bloquear IPs sospechosas o cerrar sesiones comprometidas).

**2. Funciones del Sistema de Detección de Ataques**

El **sistema de detección** de ciberataques (IDS - *Intrusion Detection System*) tiene varias funciones clave:

1. **Monitoreo en Tiempo Real:** Supervisar constantemente el tráfico y los eventos de la plataforma.
2. **Análisis de Logs:** Revisar los registros de actividad para identificar patrones inusuales.
3. **Detección de Anomalías:** Identificar comportamientos que no se alinean con la actividad normal del usuario.
4. **Reglas de Firma:** Comparar eventos con una base de datos de patrones conocidos de ataques (como firmas de ataques SQL o XSS).
5. **Alertas y Notificaciones:** Enviar alertas automáticas a los administradores cuando se detecte un posible ataque.
6. **Mitigación de Amenazas:** Aplicar bloqueos o restricciones (por ejemplo, bloquear IPs sospechosas o cerrar sesiones comprometidas).

### 3. ****Aplicación de la Poda Alfa-Beta en Seguridad****

La **poda alfa-beta** es una técnica de optimización utilizada en algoritmos de búsqueda (como Minimax) para reducir la cantidad de nodos explorados en un árbol de decisiones. Se usa principalmente en inteligencia artificial para juegos, pero su concepto también puede aplicarse en **sistemas de detección de ciberataques**.

### ****Cómo se aplicaría en la**** 3. Aplicación de la Poda Alfa-Beta en Seguridad

La **poda alfa-beta** es una técnica de optimización utilizada en algoritmos de búsqueda (como Minimax) para reducir la cantidad de nodos explorados en un árbol de decisiones. Se usa principalmente en inteligencia artificial para juegos, pero su concepto también puede aplicarse en **sistemas de detección de ciberataques**.

**Cómo se aplicaría en la detección de ataques:**

* En un contexto de detección de ciberataques, cada nodo del árbol de decisión podría representar un **evento sospechoso** o una **posible acción del sistema**.
* **Poda alfa-beta** ayuda a **descartar caminos irrelevantes** en la toma de decisiones del sistema, priorizando los eventos más críticos.
* Por ejemplo, si un evento A ya muestra una **evidencia alta de ataque**, no es necesario analizar eventos menos críticos en paralelo.
* Esto optimiza la respuesta del sistema, permitiendo reaccionar más rápido a los ataques graves sin perder tiempo en rutas menos relevantes.