

Manual de Implementación

OctoMatrix como Middleware de Validación de Eventos

1. Propósito del Documento

Este manual describe los pasos técnicos y conceptuales necesarios para implementar **OctoMatrix** como un middleware de validación de eventos dentro de una arquitectura basada en productores y consumidores. El documento está diseñado para entornos académicos, de laboratorio y prototipos controlados, priorizando claridad arquitectónica sobre optimizaciones de producción.

OctoMatrix ****no reemplaza**** mecanismos de seguridad existentes; actúa como una ****capa adicional de correlación y observabilidad**** entre comportamiento de red e intención de aplicación.

2. Alcance de la Implementación

La implementación descrita cubre:

- * Validación de eventos a nivel de aplicación usando modelos entrenados (archivo `.pkl`).
- * Correlación básica entre identidad de red (IP/MAC) y acciones observadas.
- * Integración lógica con aplicaciones existentes (ej. Parchate Pereira).

Fuera de alcance:

- * Inspección profunda de paquetes (DPI).
- * Reemplazo de sistemas IAM, ACLs o firewalls.
- * Ambientes productivos de alta criticidad.

3. Componentes del Sistema

3.1 Aplicación (Parchate Pereira)

<https://github.com/SPotes22/Pereira-Explorer-AI-Parchate-Pereira>

The screenshot displays the Pereira Explorer AI application interface, which is divided into several sections:

- Estadísticas de Eventos:** This section provides a summary of event statistics. It includes two cards: "Total Eventos" with a value of 8, and "Eventos Gratis" with a value of 7. Below these, there is a card for "Eventos Pagos" with a value of 1. A "Por Categoría:" section lists event counts by category: baile: 1, cine: 1, cultura: 3, feria: 1, gastronomia: 1, and musica: 1. An "Actualizar Stats" button is located at the bottom of this section.
- Búsqueda Avanzada:** This section features a search bar with the text "alert(1)". Below the search bar are several category filters: Música, Cine, Gastronomía, Teatro, and Ferias. At the bottom of this section are two buttons: "Buscar Eventos" and "Ver Todos".
- Eventos Reales de Pereira:** This section displays the search results for "alert(1)". It shows a message: "Resultados para 'alert(1)'" followed by "No se encontraron eventos".
- HelpBoy con Data Real:** This section includes a search bar with the text "alert(1)". Below the search bar is a button labeled "Obtener Recomendación Inteligente". Below this button, there is a section titled "Basado en tu interés, te recomiendo estos eventos:". It lists two recommended events: "Festival Internacional de Poesía Luna de Locos" (categorized as cultura) and "Convivencia Eje Rock 2025" (categorized as musica). The first event is described as the XIX edition of the international poetry festival, held on 2025-08-25 from 18:00 at the Teatro Área Cultural Cámara de Comercio de Pereira, and it is free.
- Premium MBA Service:** This section features a search bar with the text "festivales de música alternativa con bandas emergentes". Below the search bar is a button labeled "Obtener Recomendación Premium". Below this button is a button labeled "Probar Ejemplos". Below these buttons, there is a section titled "Ejemplo cargado: 'festivales de música alternativa con bandas emergentes'". It includes a message: "Ahora haz click en 'Obtener Recomendación Premium'".

<https://pereira-explorer-ai-parchate-pereira.onrender.com/>

Dec 31									
04:04:52 PM	[rhrkz]	10.203.25.224	- -	[31/Dec/2025:21:04:52 +0000]	"GET / HTTP/1.1"	200	20823	- -	"Render/1.0"
04:04:57 PM	[rhrkz]	10.203.25.224	- -	[31/Dec/2025:21:04:57 +0000]	"GET / HTTP/1.1"	200	20823	- -	"Render/1.0"
04:05:02 PM	[rhrkz]	10.203.25.224	- -	[31/Dec/2025:21:05:02 +0000]	"GET / HTTP/1.1"	200	20823	- -	"Render/1.0"
04:05:07 PM	[rhrkz]	10.203.25.224	- -	[31/Dec/2025:21:05:07 +0000]	"GET / HTTP/1.1"	200	20823	- -	"Render/1.0"
04:05:09 PM	[rhrkz]	✓ Data cargada: 8 eventos procesados							
04:05:09 PM	[rhrkz]	127.0.0.1	- -	[31/Dec/2025:21:05:09 +0000]	"GET /api/events/search?q=--admin HTTP/1.1"	200	71	"https://p...	
04:05:12 PM	[rhrkz]	10.203.25.224	- -	[31/Dec/2025:21:05:12 +0000]	"GET / HTTP/1.1"	200	20823	- -	"Render/1.0"
04:05:12 PM	[rhrkz]	10.203.25.224	- -	[31/Dec/2025:21:05:12 +0000]	"GET / HTTP/1.1"	200	20823	- -	"Render/1.0"
04:05:17 PM	[rhrkz]	10.203.25.224	- -	[31/Dec/2025:21:05:17 +0000]	"GET / HTTP/1.1"	200	20823	- -	"Render/1.0"
04:05:22 PM	[rhrkz]	10.203.25.224	- -	[31/Dec/2025:21:05:22 +0000]	"GET / HTTP/1.1"	200	20823	- -	"Render/1.0"
04:05:24 PM	[rhrkz]	✓ Data cargada: 8 eventos procesados							
04:05:24 PM	[rhrkz]	127.0.0.1	- -	[31/Dec/2025:21:05:24 +0000]	"GET /api/events/search?q=alert(1) HTTP/1.1"	200	72	"https://p...	
04:05:27 PM	[rhrkz]	10.203.25.224	- -	[31/Dec/2025:21:05:27 +0000]	"GET / HTTP/1.1"	200	20823	- -	"Render/1.0"
04:05:32 PM	[rhrkz]	10.203.25.224	- -	[31/Dec/2025:21:05:32 +0000]	"GET / HTTP/1.1"	200	20823	- -	"Render/1.0"
04:05:37 PM	[rhrkz]	10.203.25.224	- -	[31/Dec/2025:21:05:37 +0000]	"GET / HTTP/1.1"	200	20823	- -	"Render/1.0"
04:05:42 PM	[rhrkz]	10.203.25.224	- -	[31/Dec/2025:21:05:42 +0000]	"GET / HTTP/1.1"	200	20823	- -	"Render/1.0"
04:05:42 PM	[rhrkz]	10.203.25.224	- -	[31/Dec/2025:21:05:42 +0000]	"GET / HTTP/1.1"	200	20823	- -	"Render/1.0"
04:05:47 PM	[rhrkz]	10.203.25.224	- -	[31/Dec/2025:21:05:47 +0000]	"GET / HTTP/1.1"	200	20823	- -	"Render/1.0"

La aplicación cliente es responsable de:

- * Generar eventos de negocio.
- * Consumir decisiones de validación emitidas por OctoMatrix.
- * No contiene lógica de seguridad predictiva.

Archivos de referencia:

- * `app.py`
- * `brain.py`

3.2 OctoMatrix Core

OctoMatrix es el componente encargado de:

- * Cargar el modelo entrenado (`pkl`).
- * Recibir eventos normalizados.
- * Evaluar patrones y emitir decisiones (válido / sospechoso).

Archivo de referencia:

- * `octomatrix_poc_moe_owasp.py`
- <https://www.kaggle.com/code/santiagopotes/octomatrix-poc-moe-owasp/log>

3.3 Modelo de Machine Learning

El modelo entrenado:

- * Fue generado offline.
- * Presenta una precisión superior al 82%.
- * No se entrena en tiempo real.

El modelo se carga en memoria al iniciar OctoMatrix.

4. Flujo General de Implementación

1. La aplicación genera un evento.
 2. El evento se normaliza (estructura JSON o dict).
 3. El evento se envía a OctoMatrix.
 4. OctoMatrix evalúa el evento usando el modelo.
 5. Se retorna una decisión.
 6. La aplicación actúa según la decisión.
-

5. Requisitos del Entorno

5.1 Software

- * Python 3.9+
- * Librerías estándar de ML (según entrenamiento previo)
- * Entorno virtual recomendado

5.2 Hardware

- * CPU estándar (no GPU requerida)
 - * Mínimo 4 GB RAM
-

6. Preparación del Entorno

1. Crear entorno virtual.
2. Instalar dependencias.
3. Ubicar el archivo `.pkl`` en la ruta definida.
4. Verificar permisos de lectura.

7. Inicialización de OctoMatrix

Al iniciar OctoMatrix:

- * Se carga el modelo en memoria.
- * Se validan estructuras internas.
- * El sistema queda en modo escucha.

Recomendación: inicializar una sola vez por proceso.

8. Integración con la Aplicación

La aplicación debe:

- * Invocar a OctoMatrix como servicio o módulo.
- * Enviar eventos estructurados.
- * Interpretar la respuesta sin lógica adicional.

OctoMatrix ****no decide acciones finales****, solo emite evaluaciones.

9. Manejo de Resultados

Las respuestas posibles incluyen:

- * Evento válido.
- * Evento sospechoso.

La aplicación decide:

- * Registrar.
 - * Bloquear.
 - * Alertar.
-

10. Buenas Prácticas

- * Mantener el modelo desacoplado del código.
 - * No modificar el `.pkl` en caliente.
 - * Registrar decisiones para análisis posterior.
 - * No asumir falsos positivos como errores.
-

11. Limitaciones Conocidas

- * Dependencia de calidad del entrenamiento.
- * No detección de ataques completamente nuevos.
- * No reemplaza validaciones determinísticas.

12. Extensiones Futuras

- * Correlación con identidad de red (MAC/IP).
 - * Integración con Kafka.
 - * Uso de métricas SNMP.
 - * Soporte multi-modelo.
-

13. Consideraciones Académicas

Este manual está diseñado para facilitar:

- * Reproducción del experimento.
- * Evaluación técnica en laboratorio.
- * Discusión arquitectónica.

No pretende ser una guía de despliegue comercial.

14. Cierre

OctoMatrix debe entenderse como una **capa experimental de validación**, útil para explorar nuevas formas de correlacionar comportamiento, identidad y eventos sin comprometer la arquitectura existente.