Defensa Activa de Infraestructura Crítica

Ecosistema Brios

Nuestros Sistemas de defensa garantizan Soberanía Táctica Cibernética:

Agentes

- Guardian
- Vanguard
- Vanguard **+**

Infraestructura

- Centro de Operaciones
- Red-Team
- Centro de Inteligencia

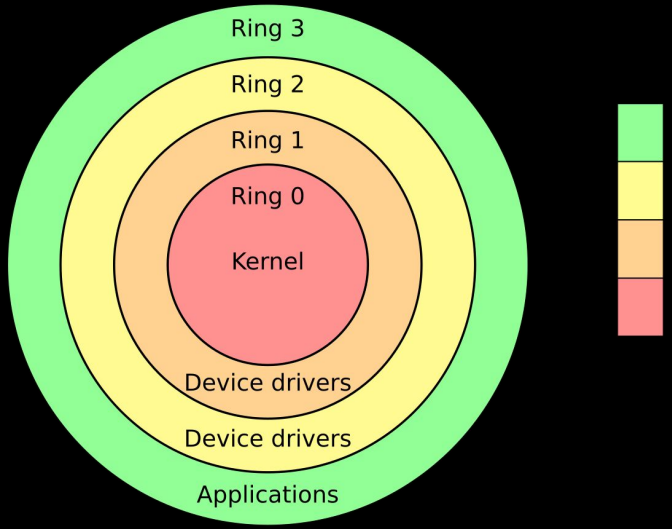
La Evolución de la Amenaza.

Los atacantes ya no usan virus en discos duros. El espionaje y el sabotaje moderno ocurren en la memoria volátil y a través de tráfico encriptado, bajo procesos legítimos.

Ataques de día cero en aumento.

Punto Ciego Operativo.

Qué pasa con un ataque que vive en RAM?

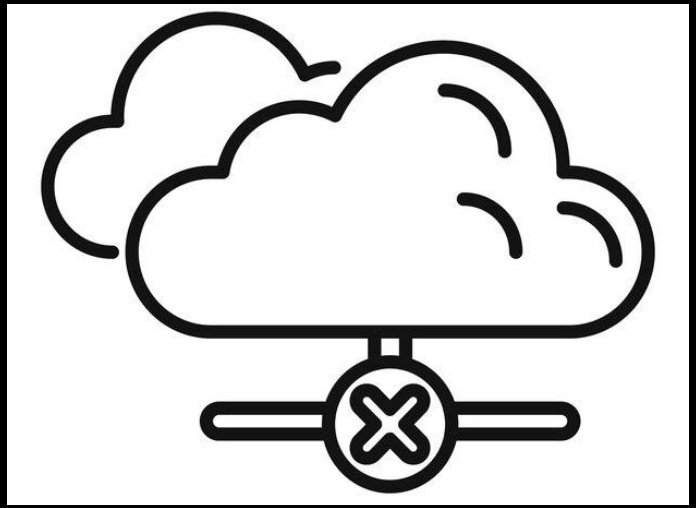


Qué pasa con un ataque que se origina de un proceso legítimo?

Las soluciones de mercado operan en "anillos" superficiales. Cuando un ataque es *Fileless* (sin archivo) o de Día Cero, las defensas convencionales quedan ciegas.

Soberanía Tecnológica y Confianza Cero.

A dónde va la telemetría?



La vigilancia genera nuevos puntos de fuga?

El ejército no puede depender de telemetría enviada a nubes extranjeras.
Brios ofrece control total, inteligencia local y capacidad de operar en redes cerradas de máxima seguridad

Arsenal Táctico:

- Brios Guardian (Nucleo)
- Vanguard (Perímetro)
- Red-Team (Reserva)
- SOC (Centro Táctico)
- Centro de Inteligencia (Reacción)

Brios Guardian: Defensa Profunda en eBPF.

24 sistemas de defensa en el kernel.

Capacidades Críticas de Contención y Neutralización:

- **Bloqueo de Hardware a Velocidad de Cable (XDP L3)**
- **Barricada Estructural Inquebrantable (Módulo LSM)**

Brios Guardian: Defensa Profunda en eBPF.

24 sistemas de defensa en el kernel.

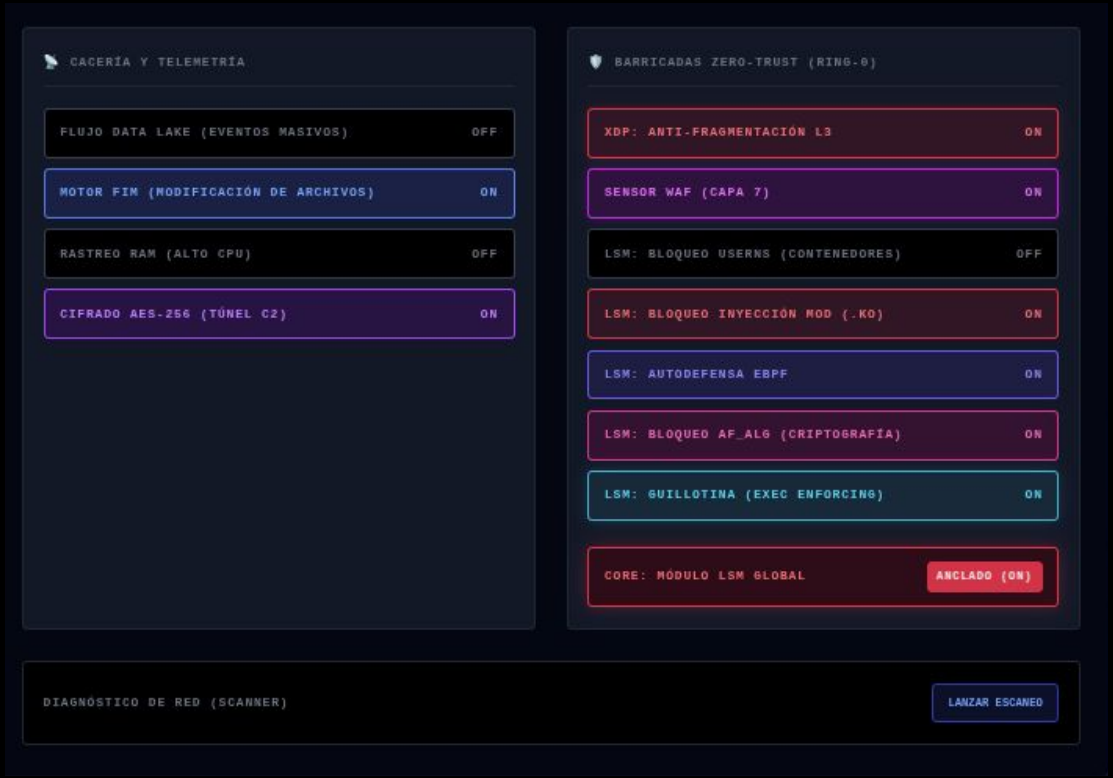
Capacidades Críticas de Contención y Neutralización:

- **Protocolo de Congelamiento Absoluto (*Freeze-and-Dump*)**
- **Aniquilación Profunda de procesos**

Bóvedas de Control de Alta Velocidad.

El sistema no consulta bases de datos lentas durante un ataque.

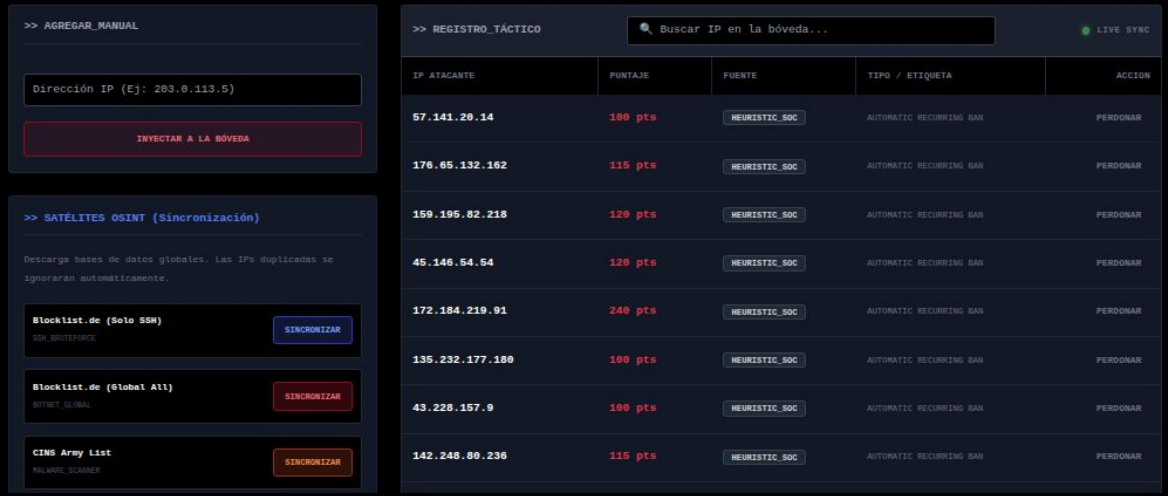
Utiliza mapas de memoria compartida ultrarrápidos inyectados en el Kernel para decisiones en microsegundos.



El Escudo de Hardware (XDP)

Escudo a nivel de Hardware: Control total en capa 3 a máxima velocidad teórica.

Mitigación de ataques volumétricos (DDoS). Fulmina IPs hostiles directamente en la tarjeta de red física, sin consumir CPU del servidor.



La Barricada Estructural LSM

Módulo LSM: El Candado del Sistema.

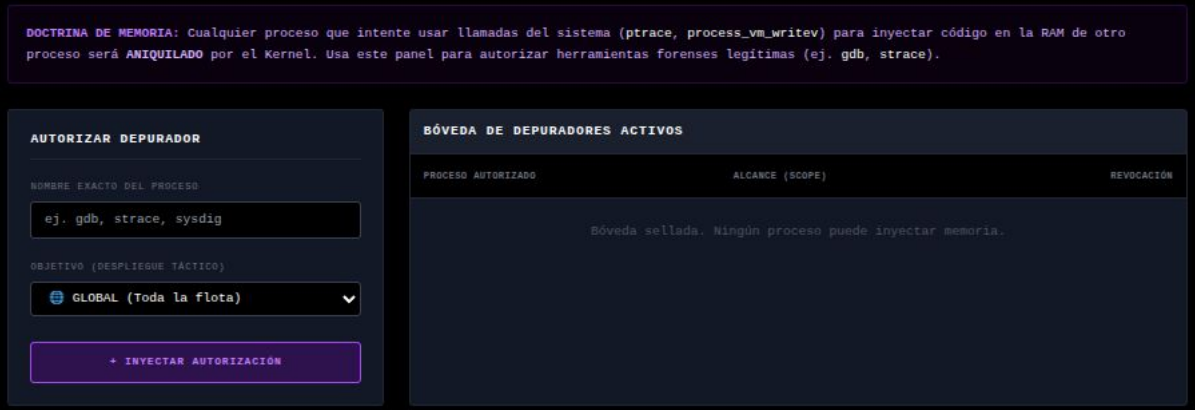
Engranajes del Kernel bloqueados (KMOD, USERNS, AF_ALG).

Le quita el poder incluso al usuario ROOT. Impide inyección de módulos (Rootkits), manipulación de criptografía y evasión de contenedores.

La Guillotina Anti-Fileless

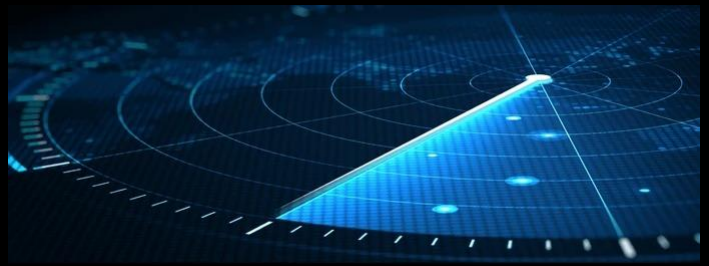
Exec Shield:
Neutralización de Ataques en RAM.

Detecta y destruye ataques "Living off the Land" y binarios volátiles antes de que el procesador ejecute su primera instrucción.



Cazador de Persistencia (FIM)

Radar de Integridad de Archivos.



Vigila rutas críticas mediante la API fanotify del Kernel. Detecta modificaciones silenciosas de configuraciones o binarios.

Laboratorio Heurístico YARA

Análisis Profundo al Vuelo (Fast-Mode)

Escanea el interior de los archivos en milisegundos buscando fragmentos de código malicioso.

Aplicación de Actualización en RAM para actualizar inteligencia sin reiniciar servidores y con propagación a toda la flota.

Protocolo Zero-Trust (Freeze-and-Dump)

Protocolo de Congelamiento Absoluto.

- El activo más valioso. Si el escaneo da positivo, el atacante es decapitado sin haber consumido un solo recurso.

- Marcado Táctico (Tagging): Todo archivo nuevo o modificado es considerado "Sucio" por defecto bajo la doctrina de Confianza Cero.

- Triaje Automatizado (Vida o Muerte): Interrogatorio heurístico en RAM (Motor YARA). Resulta en inmunidad diplomática o decapitación inmediata.

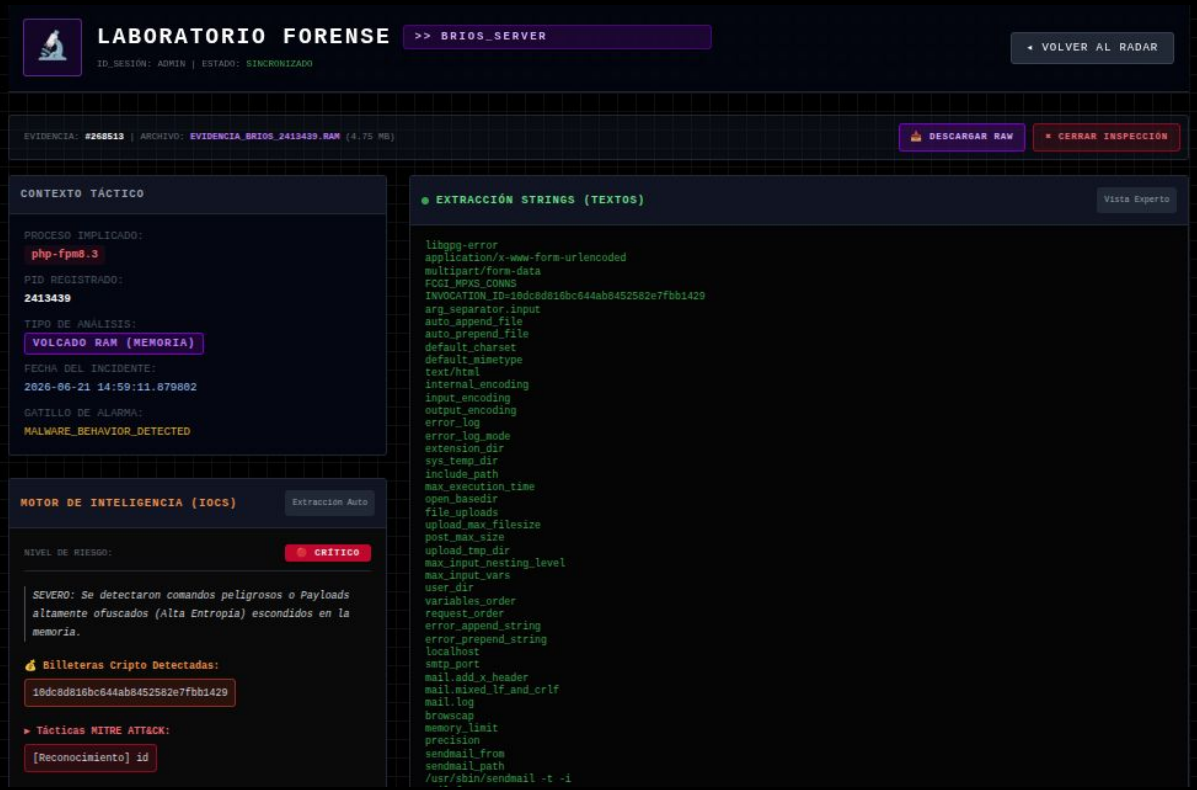
Maniobras y Fuego Real

Vigilancia de archivos

Monitoreo de Honeytokens

Volcados de RAM y RED

Laboratorio Forense RAM y RED



Brios Vanguard: agentes en Capa 7

Vanguard y Vanguard**+**

Creado para entornos shared hosting. No tenemos competencia

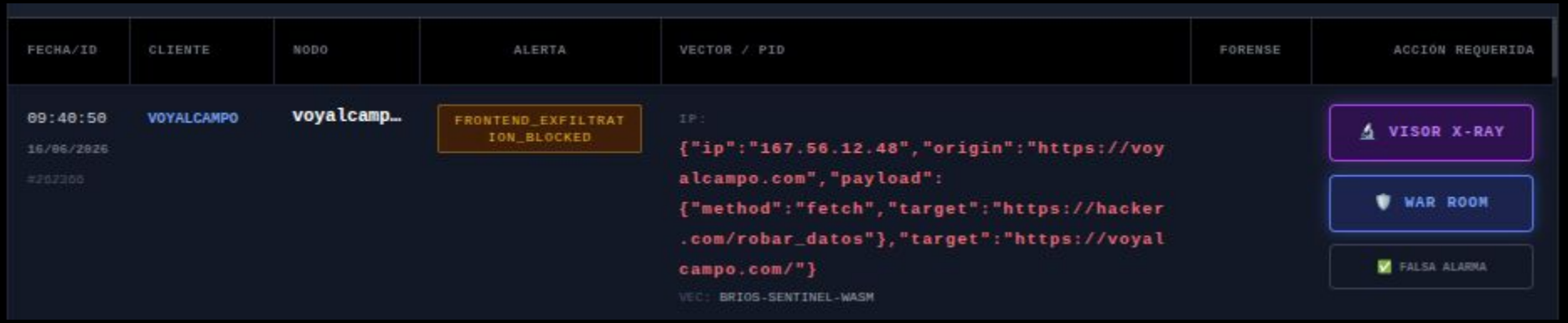
- Vigilancia de archivos
- Inserción de señuelos
- WAF ultrarrápido
- Escudo YARA
- WASM

Vanguard+ (WASM): Protección en Territorio Enemigo.

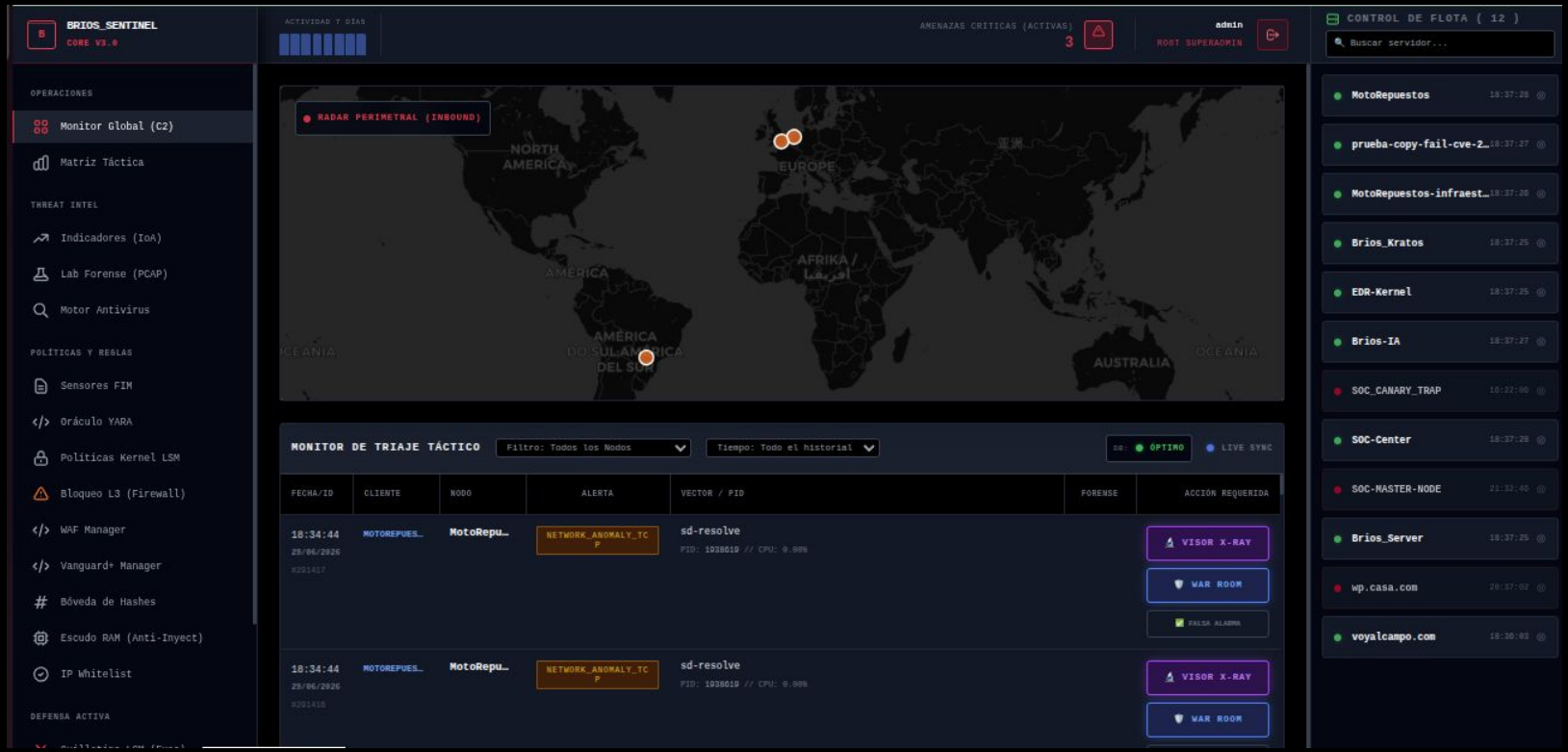
Extender la seguridad fuera del servidor militar, directamente hacia el navegador del personal que accede a los sistemas.

Vanguard+ (WASM): Protección en Territorio Enemigo.

Extender la seguridad fuera del servidor militar, directamente hacia el navegador del personal que accede a los sistemas.



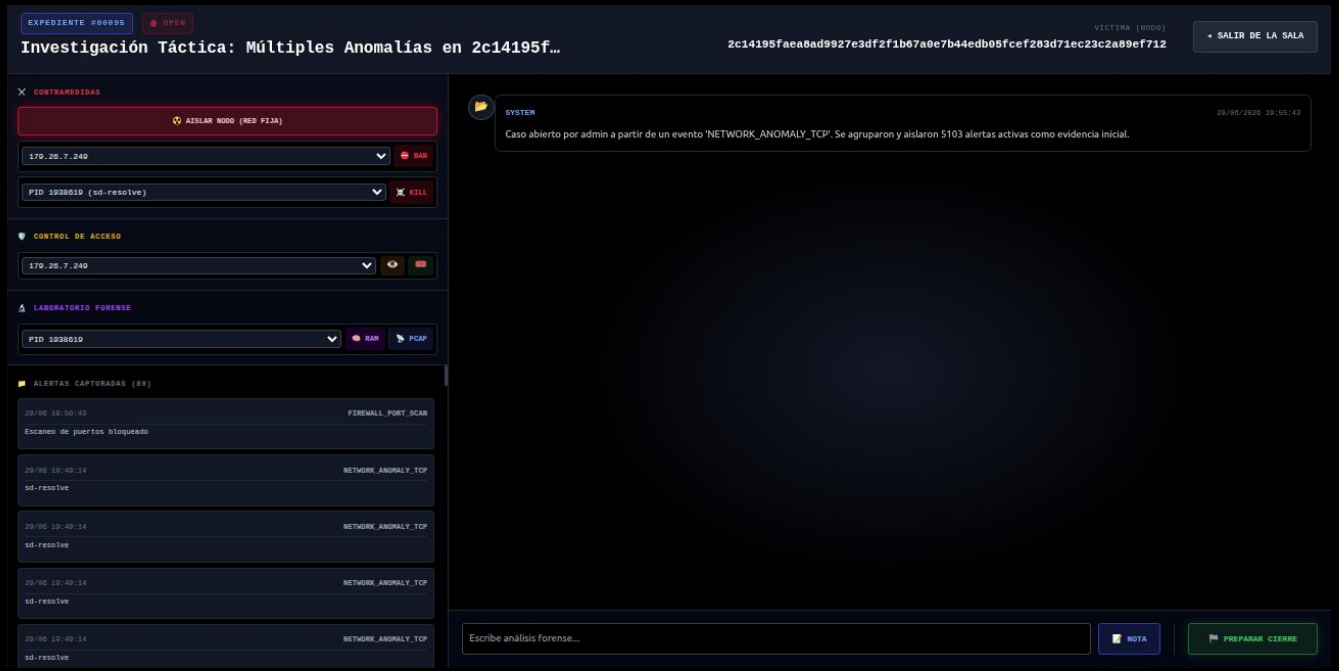
EL CENTRO DE MANDO Y CONTROL (SOC)



WAR ROOM

War Room

Agrupa incidentes, limpia el ruido visual y permite a los oficiales gestionar la crisis desde un único panel centralizado.



RESUMEN

- Soberanía Tecnológica Absoluta
- Defensa Activa en Profundidad
- Continuidad Operativa Garantizada

BRIOS CYBER SECURITY:

- 100% Libre de IA
- 100% Codigo propio
- 100% Industria Uruguaya

Alcanzar un nivel de seguridad implica previsión

En BRIOS tenemos las herramientas.

Gracias!