



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

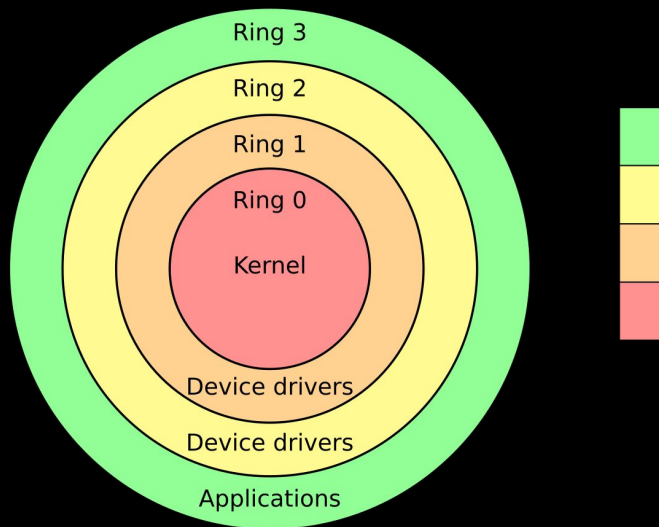
La Evolución de la Amenaza.

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?

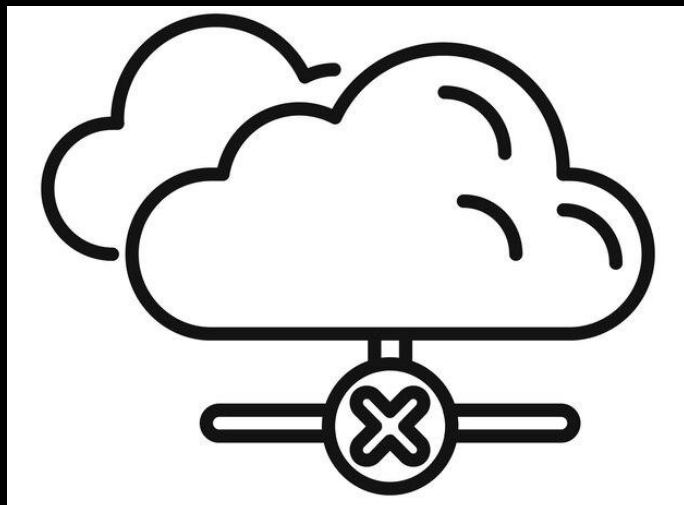


Qué pasa con un ataque que se origina de un proceso legítimo?

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** (Núcleo)
- **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.

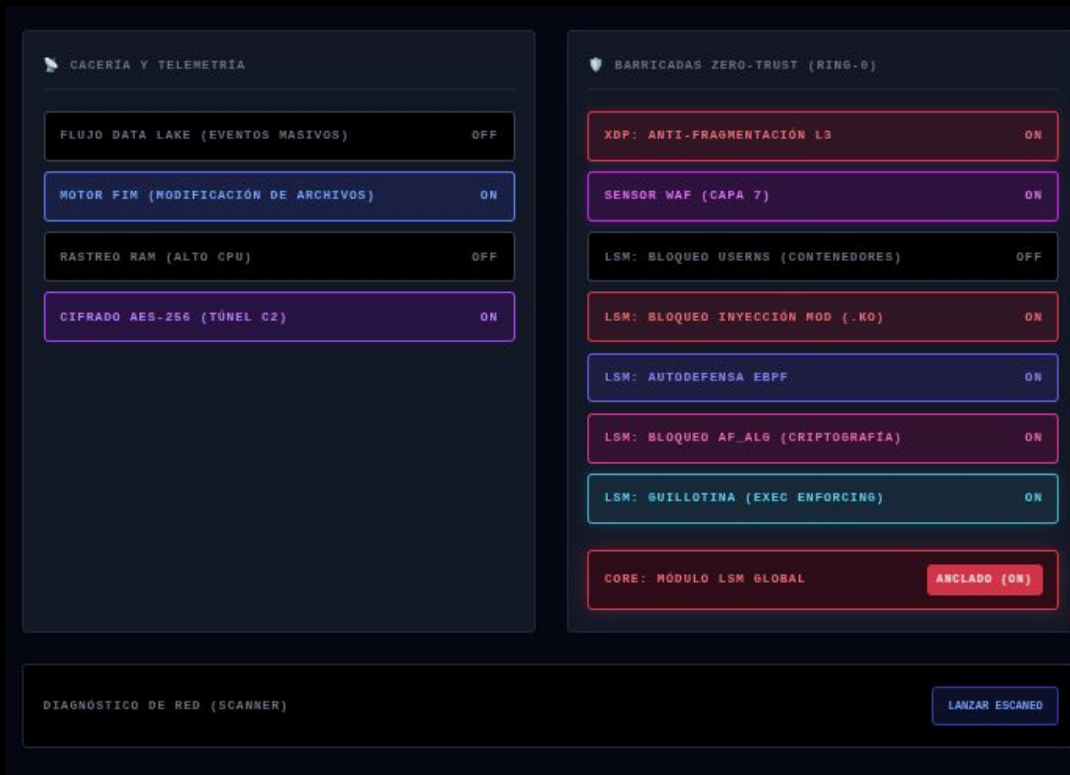
Capacidades Críticas de Contención y Neutralización:

- **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.



The screenshot displays a control interface for high-speed security controls, organized into two main panels:

- CACERÍA Y TELEMETRÍA (Hunting and Telemetry):**
 - FLUJO DATA LAKE (EVENTOS MASIVOS): OFF
 - MOTOR FIM (MODIFICACIÓN DE ARCHIVOS): ON
 - RASTREO RAM (ALTO CPU): OFF
 - CIFRADO AES-256 (TÚNEL C2): ON
- BARRICADAS ZERO-TRUST (RING-0):**
 - XDP: ANTI-FRAGMENTACIÓN L3: ON
 - SENSOR WAF (CAPA 7): ON
 - LSM: BLOQUEO USERNS (CONTENEDORES): OFF
 - LSM: BLOQUEO INYECCION MOD (.KO): ON
 - LSM: AUTODEFENSA EBPF: ON
 - LSM: BLOQUEO AF_ALG (CRIPTOGRAFÍA): ON
 - LSM: GUILLOTINA (EXEC ENFORCING): ON
 - CORE: MÓDULO LSM GLOBAL: ANCLADO (ON)

At the bottom, there is a section for **DIAGNÓSTICO DE RED (SCANNER)** with a **LANZAR ESCANEADO** button.

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.

>> AGREGAR MANUAL

Dirección IP (Ej: 203.0.113.5)

INYECTAR A LA BÓVEDA

>> SATÉLITES OSINT (Sincronización)

Descarga bases de datos globales. Las IPs duplicadas se ignorarán automáticamente.

BlockList.de (Solo SSH) SIN BRUTEFORCE SINCRONIZAR

BlockList.de (Global All) BOTNET, SCIBOT SINCRONIZAR

CINS Army List HWLWARE_SCANNER SINCRONIZAR

>> REGISTRO TÁCTICO Buscar IP en la bóveda... LIVE SYNC

IP ATACANTE	PUNTAJE	FUENTE	TIPO / ETIQUETA	ACCION
57.141.20.14	100 pts	HEURISTIC_SOC	AUTOMATIC RECURRING BAN	PERDONAR
176.65.132.162	115 pts	HEURISTIC_SOC	AUTOMATIC RECURRING BAN	PERDONAR
169.195.82.218	120 pts	HEURISTIC_SOC	AUTOMATIC RECURRING BAN	PERDONAR
46.146.54.54	120 pts	HEURISTIC_SOC	AUTOMATIC RECURRING BAN	PERDONAR
172.184.219.91	240 pts	HEURISTIC_SOC	AUTOMATIC RECURRING BAN	PERDONAR
135.232.177.180	100 pts	HEURISTIC_SOC	AUTOMATIC RECURRING BAN	PERDONAR
43.228.167.9	100 pts	HEURISTIC_SOC	AUTOMATIC RECURRING BAN	PERDONAR
142.248.80.236	115 pts	HEURISTIC_SOC	AUTOMATIC RECURRING BAN	PERDONAR

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.

DOCTRINA DE MEMORIA: Cualquier proceso que intente usar llamadas del sistema (ptrace, process_vm_writev) para inyectar código en la RAM de otro proceso será ANIQUILADO por el Kernel. Usa este panel para autorizar herramientas forenses legítimas (ej. gdb, strace).

AUTORIZAR DEPURADOR

NOMBRE EXACTO DEL PROCESO

ej. gdb, strace, sysdig

OBJETIVO (DESPLIEGUE TÁCTICO)

GLOBAL (Toda la flota)

+ INYECTAR AUTORIZACIÓN

BÓVEDA DE DEPURADORES ACTIVOS

PROCESO AUTORIZADO

ALCANCE (SCOPE)

REVOCACIÓN

Bóveda sellada. Ningún proceso puede inyectar memoria.

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.
- Triage 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

ESTADO DEL NODO
● SISTEMA_ACTIVO


BRIOS // MATRIZ TÁCTICA

>> Brios_Server
 AISLAR NODO (RED)
◀ Volver al Radar

ID_SESION: ADMIN | VISTO: 21:23:12

MOTOR HEURÍSTICO

CPU
RAM



VIGÍA FIM

FIM_VIOLATION 08:20:23
 Modificado /usr/bin/xdx
 PID: 2311963 EJE: SISTEMA/DRIVERS

FIM_VIOLATION 08:20:23
 Modificado /usr/bin/vimtutor
 PID: 2311963 EJE: SISTEMA/DRIVERS

FIM_VIOLATION 08:20:23

HONEYTOKENS

¡INTRUSIÓN DETECTADA EN CEB0!

FREEZE_DUMP_CLEARED
 [00:00:03]

 YOT: Auditoría Limpia: Inmunidad otorgada a /usr/bin/tar

 Linaje: dpkg-db-backup (2462865) < dpkg-db-backup (2461987) < systemd (1)

 Atacante PID: 2462865

FREEZE_DUMP_CLEARED
 [00:00:03]

 YOT: Auditoría Limpia: Inmunidad otorgada a /usr/b

RADAR TCP

>> Escáner de Sockets Activo...
 > Ninguna anomalía detectada.

BÓVEDA FORENSE

21/06 14:39:11 PID_Culpable: 2413439

 RED (-pcap) DL ANALIZAR

 MEMORIA (-ram) DL ANALIZAR

21/06 14:30:44 PID_Culpable: 2413258

 RED (-pcap) DL ANALIZAR

 MEMORIA (-ram) DL ANALIZAR

REGISTRO DE BAJAS


11/04 22:11:16

 PID: 1934 mariadb

 > 37.27.217.253

 NETWORK_ANOMALY_TCP ID_BALA: #31

Laboratorio Forense RAM y RED



LABORATORIO FORENSE >> BRIOS_SERVER

VOLVER AL RADAR

EVIDENCIA: #268513 | ARCHIVO: EVIDENCIA.BRIOS.2413439.RAM (4.75 MB)

DESCARGAR RAW
CERRAR INSPECCIÓN

CONTEXTO TÁCTICO

PROCESO IMPLICADO:
php-fpm@3

PID REGISTRADO:
2413439

TIPO DE ANÁLISIS:
VOLCADO RAM (MEMORIA)

FECHA DEL INCIDENTE:
2026-06-21 14:59:11.879882

GATILLO DE ALARMA:
MALWARE_BEHAVIOR_DETECTED

EXTRACCIÓN STRINGS (TEXTOS)

Vista Experto

```

libpng-error
application/x-www-form-urlencoded
multipart/form-data
FOCI.MPXS.COMMS
INVOCATION_ID=18dc8d816bc644ab8452582e7fbb1429
arg_separator.input
auto_append_file
auto_prepend_file
default_charset
default_mime_type
text/html
internal_encoding
input_encoding
output_encoding
error_log
error_log_mode
extension_dir
sys_temp_dir
include_path
max_execution_time
open_basedir
file_uploads
upload_max_filesize
post_max_size
upload_tmp_dir
max_input_nesting_level
max_input_vars
user_dir
variables_order
request_order
error_append_string
error_prepend_string
localhost
smtp_port
mail_add_x_header
mail_mixed_if_and_crlf
mail_log
Browscap
memory_limit
precision
sendmail_from
sendmail_path
/usr/sbin/sendmail -t -i
          
```

MOTOR DE INTELIGENCIA (IOCS)

Extracción Auto

NIVEL DE RIESGO: CRÍTICO

SEVERO: Se detectaron comandos peligrosos o Payloads altamente ofuscados (Alta Entropía) escondidos en la memoria.

🔍 Billeteras Cripto Detectadas:

18dc8d816bc644ab8452582e7fbb1429

► Tácticas MITRE ATTACK:

[Reconocimiento] id

Brios Vanguard: agentes en Capa 7

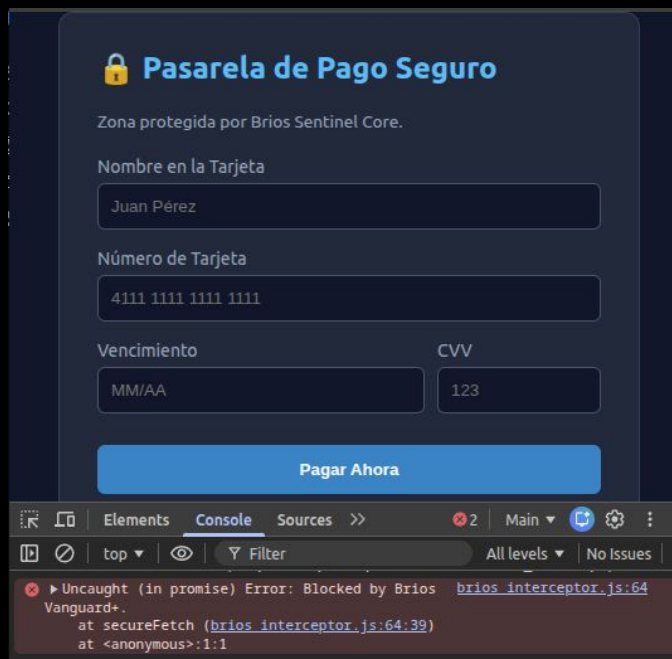
Vanguard y Vanguard+

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.

FECHA/ID	CLIENTE	NODO	ALERTA	VECTOR / PID	FORENSE	ACCIÓN REQUERIDA
09:40:50 16/06/2025 #287200	VOYALCAMPO	voyalcamp...	FRONTEND_EXFILTRAT ION_BLOCKED	IP: { "ip": "167.56.12.48", "origin": "https://voyalcampo.com", "payload": { "method": "fetch", "target": "https://hacker.com/robar_datos"}, "target": "https://voyalcampo.com/" } VEC: BRIOS-SENTINEL-WASM		VISOR X-RAY WAR ROOM <input checked="" type="checkbox"/> FALSA ALARMA

EL CENTRO DE MANDO Y CONTROL (SOC)

BRIOS SENTINEL
CORE V3.0

ACTIVIDAD Y DÍAS


AMENAZAS CRÍTICAS (ACTIVAS)
3

admin
ROOT SUPERADMIN

CONTROL DE FLOTA (12)

OPERACIONES

Monitor Global (C2)

Matriz Táctica

THREAT INTEL

Indicadores (IoA)

Lab Forense (PCAP)

Motor Antivirus

POLÍTICAS Y REGLAS

Sensores FIM

Oráculo YARA

Políticas Kernel LSM

Bloqueo L3 (Firewall)

WAF Manager

Vanguard+ Manager


Bóveda de Hashes

Escudo RAM (Anti-Inyect)

IP Whitelist

DEFENSA ACTIVA

RADAR PERIMETRAL (INBOUND)



MONITOR DE TRIAJE TÁCTICO

Filtro: Todos los Nodos Tiempo: Todo el historial

● OPTIMO ● LIVE SYNC

FECHA/ID	CLIENTE	NODO	ALERTA	VECTOR / PID	FORENSE	ACCIÓN REQUERIDA
18:34:44 29/06/2026 R021817	MOTOREPUES...	MotoRepu...	NETWORK_ANOMALY_TC P	sd-resolve PID: 1938019 // CPU: 0.00%		VISOR X-RAY WAR ROOM FALSA ALARMA
18:34:44 29/06/2026 R021818	MOTOREPUES...	MotoRepu...	NETWORK_ANOMALY_TC P	sd-resolve PID: 1938019 // CPU: 0.00%		VISOR X-RAY WAR ROOM

CONTROL DE FLOTA (12)

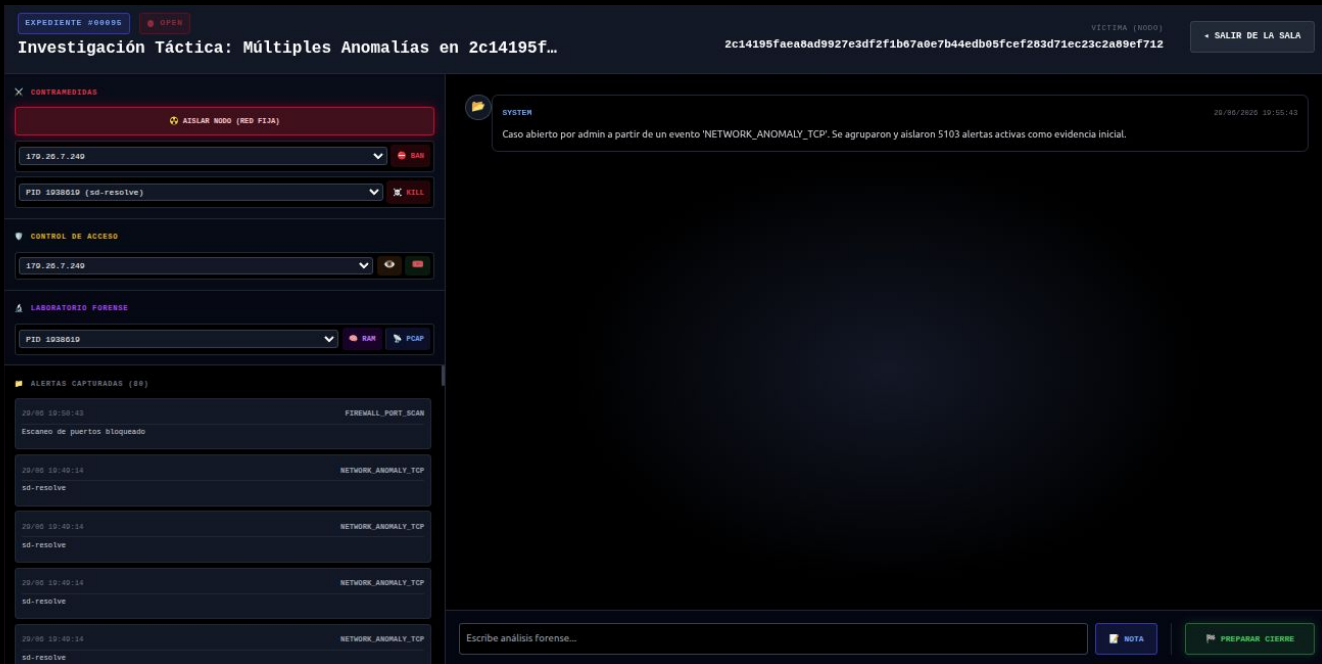
Buscar servidor...

- MotoRepuestos 18:37:28
- prueba-copy-fail-cve-2... 18:37:27
- MotoRepuestos-infraest... 18:37:26
- Brios_Kratos 18:37:25
- EDR-Kernel 18:37:25
- Brios-IA 18:37:27
- SOC_CANARY_TRAP 18:22:00
- SOC-Center 18:37:28
- SOC-MASTER-NODE 21:32:40
- Brios_Server 18:37:25
- wp.casa.com 20:37:52
- voyalcampo.com 18:30:03

WAR ROOM

War Room

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



EXPEDIENTE #00095 OPDR 2c14195faea8ad9927e3df2f1b67a0e7b44ed05fcef283d71ec23c2a89ef712 VICTIMA (NODO) + SALIR DE LA SALA

Investigación Táctica: Múltiples Anomalías en 2c14195f...

CONTRAMEDIDAS
AISLAR NODO (RED F13A)

170.26.7.240 BAR
 PID_193801D (sd-resolve) KILL

CONTROL DE ACCESO
 170.26.7.240 BAR

LABORATORIO FORENSE
 PID_193801D BAR PCAP

ALERTAS CAPTURADAS (89)

20/06 16:00:43	FIREWALL_PORT_SCAN
Escaneo de puertos bloqueado	
20/06 15:40:14	NETWORK_ANOMALY_TCP
sd-resolve	
20/06 15:40:14	NETWORK_ANOMALY_TCP
sd-resolve	
20/06 15:40:14	NETWORK_ANOMALY_TCP
sd-resolve	
20/06 15:40:14	NETWORK_ANOMALY_TCP
sd-resolve	

SYSTEM 20/06/2025 10:55:43
 Caso abierto por admin a partir de un evento 'NETWORK_ANOMALY_TCP'. Se agruparon y aislaron 5103 alertas activas como evidencia inicial.

Escribe análisis forense...
NOTA
PREPARAR CIERRE

RESUMEN

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

BRIOS CYBER SECURITY:

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

Alcanzar un nivel de seguridad implica previsión

En BRIOS tenemos las herramientas.

Gracias!