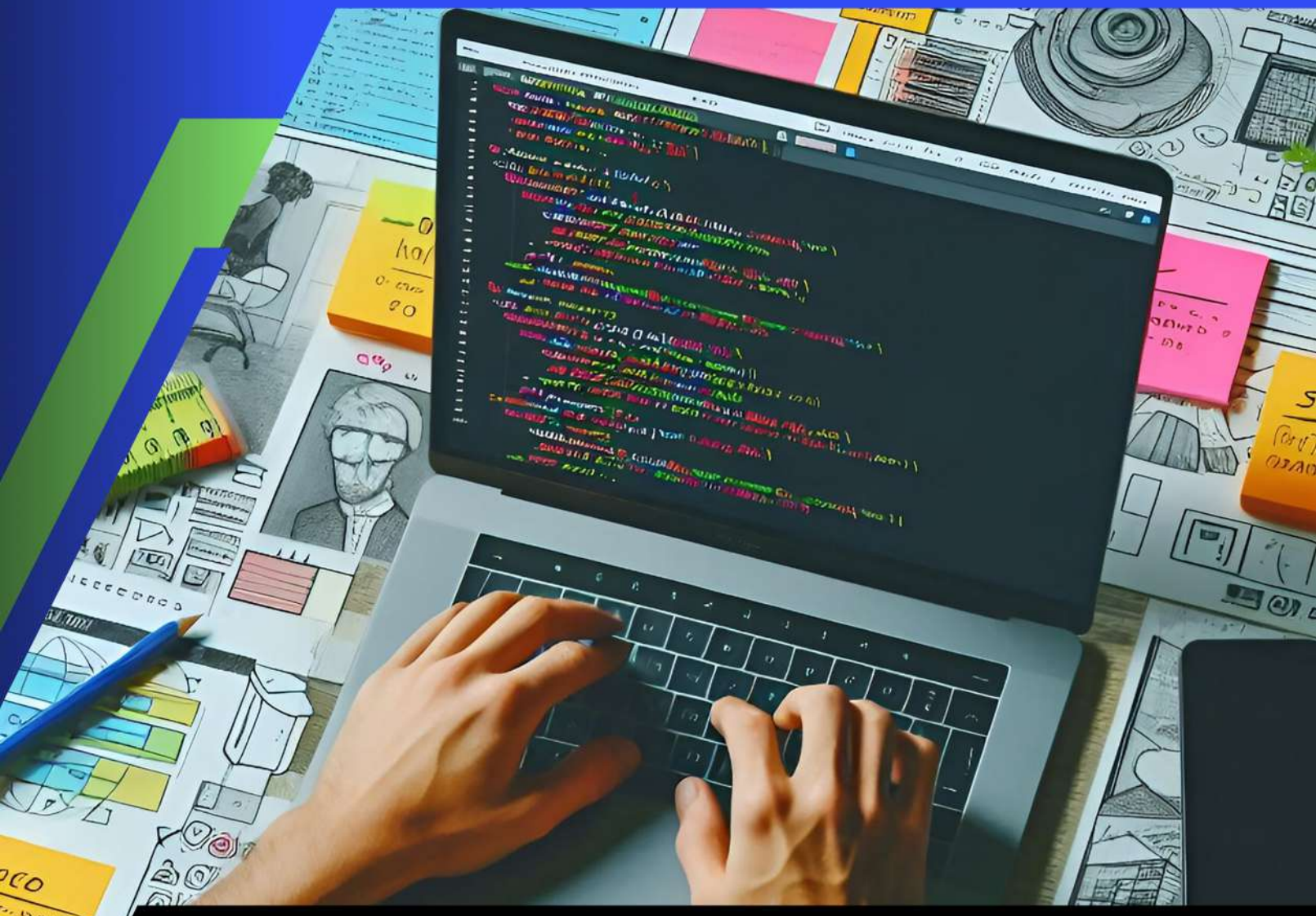
T.I RESCUE

SEGURIDAD INFORMÁTICA



Rescue
DevSecOps

www.tirescue.com
Info@tirescue.com.co
(57)315 259 2011

DISTINCIÓN EXCELENCIA

ISO 9001

Seguridad informática premium, respaldada por el reconocimiento internacional ISO 9001.

SC-CER900888

ISO 27001

Defendiendo Tus Datos con Rigor Internacional: Certificación ISO 27001.

SI-CER900889

ISO 20000-1

Excelencia en ciberseguridad, fundamentada en estándares mundiales de calidad.

TI-CER988544

ISO 22301

Continuidad del negocio sin interrupciones, conforme a estándares internacionales.

CO-CNCER988779

CUATRO CERTIFICACIONES ISO DEFINEN NUESTRA SUPERIORIDAD

Nuestro compromiso con la ciberseguridad trasciende la simple retórica. Es tangible y está validado por cuatro prestigiosas certificaciones **ISO: 9001, 27001, 20000-1 y 22301.** Estas no son solo acrónimos, sino un testimonio de nuestra dedicación para ofrecer servicios de primera clase. Representan nuestra promesa de calidad, seguridad, **eficiencia y resiliencia.** Al elegirnos, no solo está optando por un proveedor de ciberseguridad, sino por un aliado certificado que entiende y cumple con los más altos estándares internacionales.

COMPROMISO INTEGRAL: **MÁS ALLÁ DE LA SEGURIDAD BÁSICA**

Con nuestras certificaciones, garantizamos **calidad, seguridad de la información, excelencia en TI y continuidad del negocio**. Representan nuestro compromiso, profesionalismo e integridad. Elegirnos es optar por la ciberseguridad de élite y con respaldo.

icontec ISO 9001 SC-CER900888

icontec ISO / IEC 27001 SI-CER900889

icontec ISO / IEC 20000-1 TI-CER988544

icontec ISO 22301 CO-CNCER988779

IQNET CERTIFIED MANAGEMENT SYSTEM

PENTESTING AVANZADO

Certified Red Team Professional (CRTP)

Especialización en **Red Teaming** y ataques en **Active Directory**, validando técnicas avanzadas de explotación y escalamiento de privilegios en entornos empresariales.

Practical Network Penetration Tester (PNPT)

La certificación PNPT de TCM Security acredita habilidades en **pentesting real**, incluyendo explotación, escalamiento de privilegios y reportes profesionales.

Certified Ethical Hacker Master

Certificación en hacking ético y ciberseguridad ofensiva, validando habilidades en pruebas de penetración, análisis de vulnerabilidades y ataques controlados.

Cisco Ethical Hacker

Certificación en hacking ético y pruebas de penetración, con habilidades en análisis de vulnerabilidades, seguridad en redes y explotación de amenazas.

Hack The Box Pro Labs - Zephyr

Certificación avanzada en pentesting ofensivo, cubriendo ataques SQL, escalación de privilegios, explotación de aplicaciones web y movimiento lateral en redes.

Hack The Box Pro Labs - Offshore

Certificación en pentesting avanzado, con enfoque en ataques a Active Directory, evasión de protecciones, escalación de privilegios y tunneling.

Hack The Box Pro Labs - Rastalabs

Certificación en explotación de Active Directory, evasión de defensas, desarrollo de exploits y ataques de phishing, con enfoque en pentesting avanzado.

CERTIFICACIONES AVANZADAS

Certified Purple Team Analyst (CPTA V2)

Especialización en Purple Team (Red + Blue Team) Enfocado en validar controles de seguridad y mejorar la detección mediante ejercicios colaborativos.

Certified Cyber Defense Analyst (CCDA)

Especialización en Defensa Cibernética y Operación SOC Enfocado en monitoreo, correlación de eventos y análisis de alertas para detección temprana.

Certified Red Team Specialist V2 (CRTS V2)

Especialización en Red Team y Pentesting Enfocado en evaluaciones ofensivas controladas: reconocimiento, explotación y post-explotación.

Certified Web Red Team Analyst

Explotación avanzada de vulnerabilidades, **escalamiento de privilegios**, validación de impacto y documentación de hallazgos para mejorar la seguridad en entornos empresariales.

Certified Red Team Analyst (CRTA)

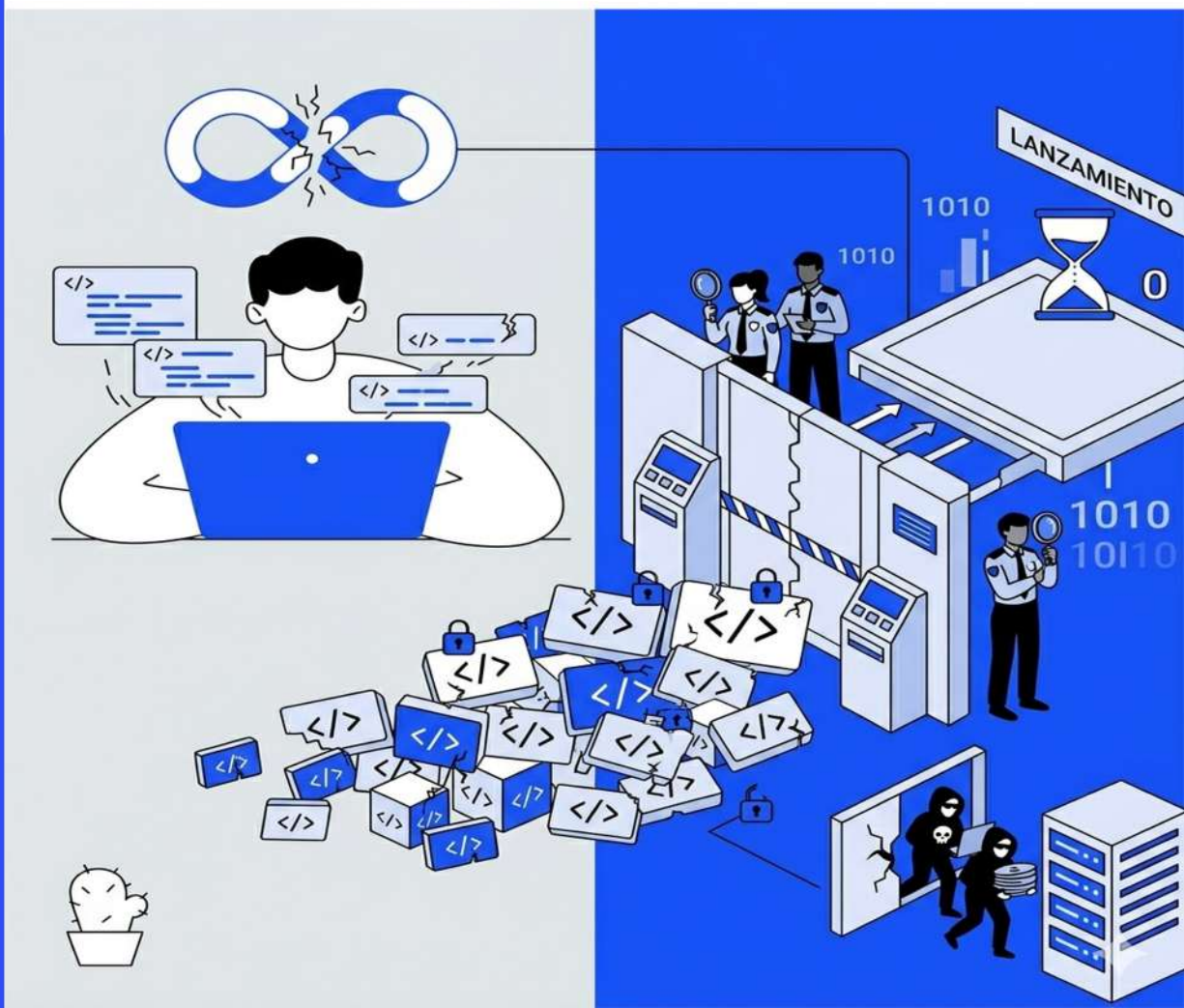
Especialización en Red Teaming y ataques en Active Directory, aplicando **técnicas avanzadas** de explotación y escalamiento de privilegios en entornos empresariales.

Blue Team Fundamentals

Fundamentos de **Blue Team y defensa en ciberseguridad**, con enfoque en monitoreo de amenazas, respuesta a incidentes y gestión de vulnerabilidades para proteger infraestructuras críticas.

¿Cómo se crea el software hoy **y por qué es un riesgo?**

Tradicionalmente, **los creadores de software y los expertos en seguridad trabajan por separado.** El equipo termina de programar y, cuando la aplicación ya está lista para salir al mercado, se le entrega a seguridad. **Si encuentran una falla grave, todo el proyecto debe frenarse y devolverse al punto de partida.** O peor aún, por el afán de cumplir fechas, el software se publica con brechas ocultas, exponiendo su negocio a ciberataques.



¿Qué problemas genera **esto en su negocio?**

www.tirescue.com

01 Vulnerabilidades

Por la presión de salir rápido al mercado, muchas empresas terminan publicando aplicaciones con **"puertas abiertas"** para los ciberdelincuentes.

02 Costos altísimos

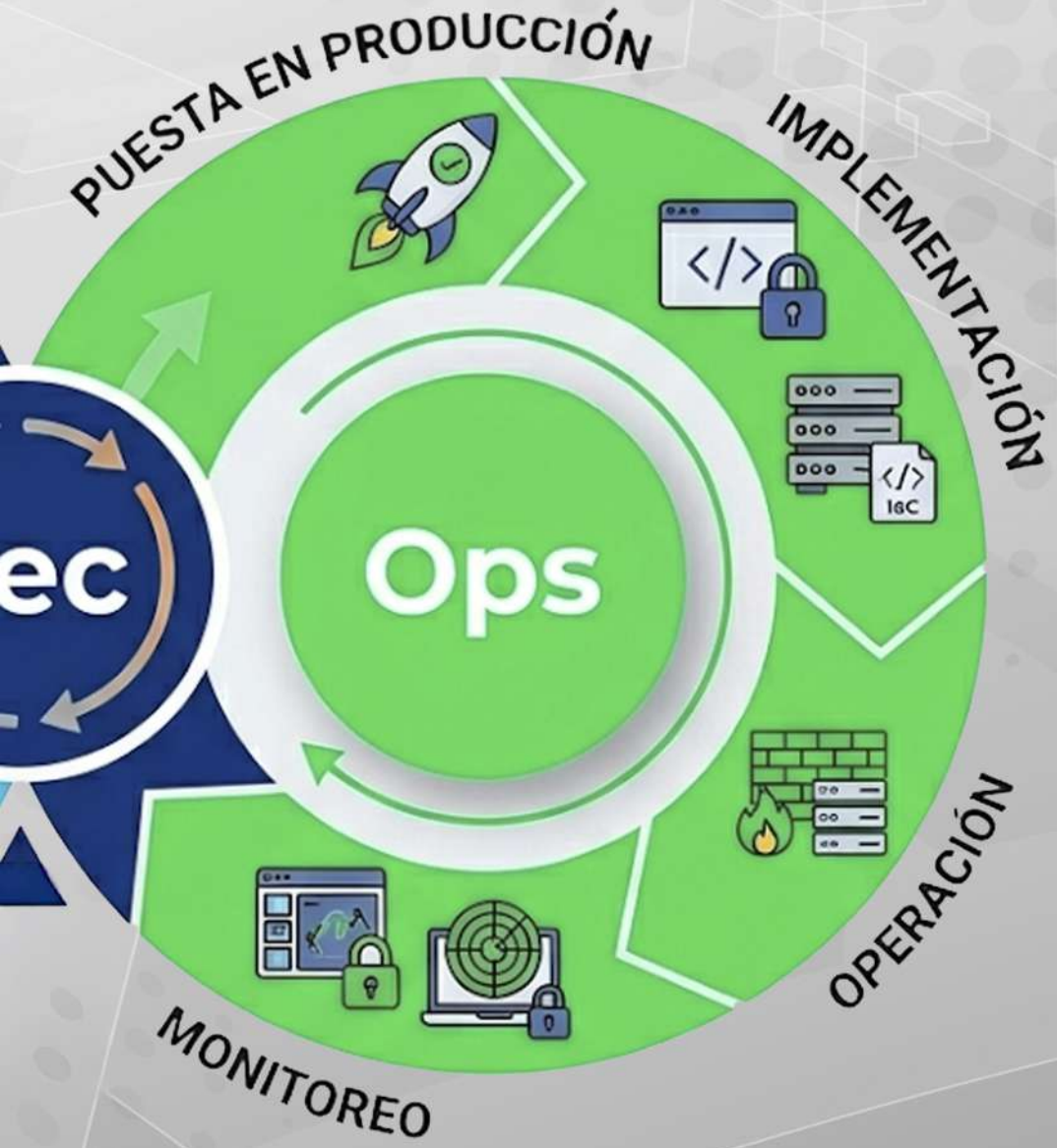
Romper paredes para arreglar una tubería mala es carísimo. En el software pasa igual: **corregir una falla cuando la aplicación ya está terminada** cuesta muchísimo más que haberla evitado al principio.

03 Frenos de emergencia

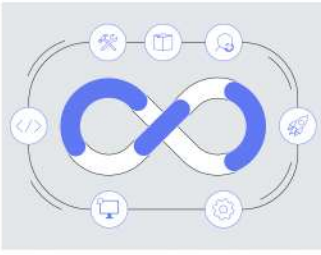
Justo cuando el producto está listo para salir a la venta, **las revisiones de seguridad detienen todo el proyecto.**

DEVSEC OPS: E
INTEGRADO

EL ECOSISTEMA
Y **UNIFICADO**



Tecnología de punta integrada en su **ADN de desarrollo**



El **Pipeline** acelera, **SAST** blinda su código y **SBOM** vigila a terceros. Protección 360° automatizada y sin interrupciones, reduciendo drásticamente los costos de remediación y acelerando su salida al mercado.

01

Pipeline CI/CD (Integración y Despliegue Continuo)

En lugar de frenar el tráfico con retenes manuales al final del camino, instalamos **controles de seguridad automatizados** que revisan todo a alta velocidad, **sin interrumpir el ritmo** de sus desarrolladores.

02

SAST (Pruebas de Seguridad Estática)

Analizamos el código mientras se está escribiendo y antes de que se compile. Esto nos permite detectar vulnerabilidades (como contraseñas expuestas o fallas lógicas) de raíz, solucionándolas cuando es más fácil y económico hacerlo.

03

SBOM (Lista de Materiales de Software)

Generamos un inventario exhaustivo de cada librería, componente de terceros y código abierto que conforma su software. **Si mañana surge una amenaza global** (como una vulnerabilidad de **"día cero"**), sabremos en segundos si su sistema está expuesto y cómo protegerlo de inmediato.

Construir con la **seguridad** integrada **desde el día uno**

01

Ahorro inteligente

Detectar y corregir una falla de seguridad **mientras apenas se está escribiendo** el código es infinitamente más barato y rápido que intentar parchar una aplicación que ya está funcionando y con clientes usándola.

02

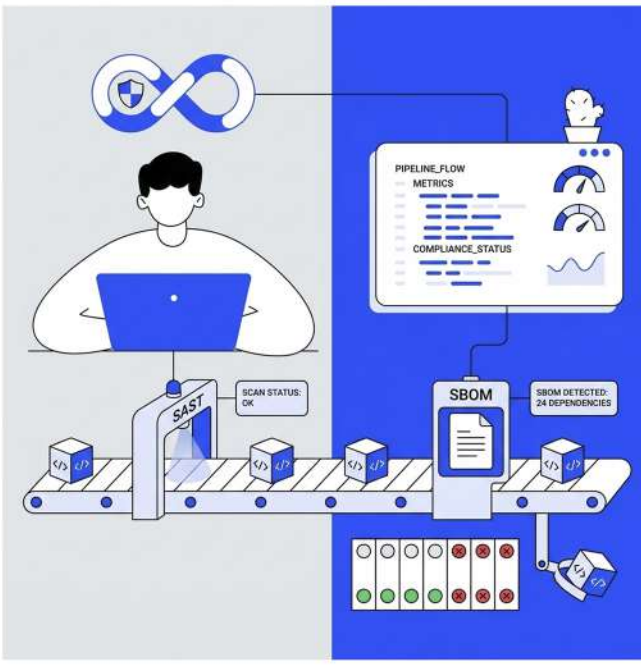
Confianza de nivel global

Respaldamos su operación con procesos estructurados y certificados bajo **normativas internacionales**, garantizando que cada línea de código cumple con los más altos estándares de protección de la información.

03

Acelerador, no freno

Automatizamos los controles de seguridad para que sus equipos sigan programando rápido, pero sin riesgos. La seguridad se vuelve invisible y deja de ser un obstáculo.



Piense en una **línea de producción moderna**. En lugar de tener a un inspector revisando el producto terminado al final del día, existen sensores de calidad que evalúan cada pieza en tiempo real mientras avanza por la cinta. Así funciona DevSecOps: **integramos la seguridad en el ADN de su software de forma automática y continua.**

Capacidades Avanzadas
DevSecOps

Protección activa antes y durante el despliegue. Ejecutamos pruebas dinámicas (DAST), auditamos scripts de infraestructura (IaC) para evitar configuraciones débiles y **bloqueamos la fuga de credenciales.**

01

DAST (Pruebas Dinámicas de Seguridad):
Auditamos la aplicación en ejecución, **simulando ataques reales** para detectar brechas que el análisis estático en el código fuente no puede ver.

02

Seguridad en IaC (Infraestructura como Código):
Evaluamos sus scripts de despliegue en la nube para garantizar que ningún servidor o base de datos nazca con puertos abiertos o configuraciones vulnerables.

03

Gestión Estricta de Secretos:
Implementamos **bloqueos automáticos** en el flujo de trabajo para evitar que credenciales, tokens o llaves de API terminen expuestos por error en sus repositorios.

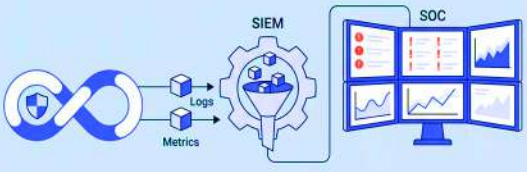
Gobernanza Automatizada y **Monitoreo Continuo**

Garantiza tranquilidad operativa. Su equipo verá un entorno donde las reglas de cumplimiento se aplican solas, **las amenazas se notifican al instante y su entorno de producción se mantiene blindado.**

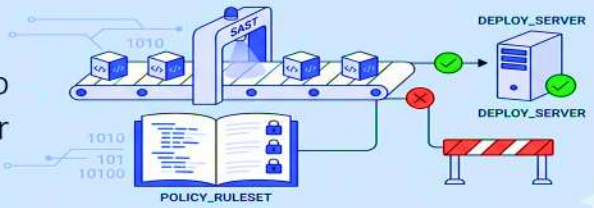
Protección a **nivel de infraestructura** con respuesta a incidentes y cumplimiento automatizado.

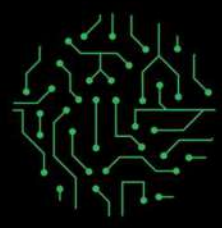
Seguridad de Contenedores
Bloqueo de vulnerabilidades en imágenes Docker y Kubernetes antes de producción.

Integración con SOC y SIEM
Envío de alertas del pipeline para correlación de **eventos y respuesta inmediata.**



Políticas como Código
Reglas de cumplimiento automatizadas para bloquear despliegues no autorizados.





T.I RESCUE

SEGURIDAD INFORMATICA

WWW.TIRESCUE.COM

Expertos en Ciberseguridad