



Secure
Tuning **iQ**

RESUMEN EJECUTIVO · PARA CISOS Y LÍDERES DE RIESGO TECNOLÓGICO

HARDENING Y CUMPLIMIENTO CONTINUO

El cumplimiento deja de ser un proyecto. Pasa a ser un estado que se mide todos los días.

Secure Tuning IQ evalúa de forma continua la configuración segura de servidores y estaciones contra CIS Benchmarks, prioriza lo que importa, guía la corrección y deja evidencia lista para su auditor.

Visibilidad

Postura real de toda la flota en un solo indicador, por unidad de negocio.

Acción

Cada desviación llega con su corrección, su responsable y su verificación.

Evidencia

Trazabilidad completa de quién cambió qué, cuándo y por qué.

La configuración insegura es la brecha que nadie está mirando entre auditorías.

Los equipos invierten en detección y respuesta, pero la línea base de sus sistemas se verifica a mano, una vez por trimestre. Entre un corte y otro, la postura cambia sin que nadie lo note.

01

Auditorías que se viven como incendios

Cada ciclo empieza de cero: recolectar evidencias, mapear hallazgos a controles y esperar que nada se haya movido desde el último corte.

02

Herramientas que no escalan

Los escáneres puntuales funcionan en diez equipos. Con cientos de hosts, varios sistemas operativos y distintas áreas, se vuelven inmanejables.

03

Hallazgos sin plan

Una hoja de cálculo con miles de reglas fallidas no es un plan de remediación. Sin prioridad ni responsable, el riesgo permanece abierto.

EL CAMBIO DE MODELO

	Enfoque tradicional	Con Secure Tuning IQ
Frecuencia	Revisión trimestral o anual	Evaluación continua y programada
Desviaciones	Se descubren en la siguiente auditoría	Se detectan el mismo día en que ocurren
Remediación	Investigación manual por cada hallazgo	Corrección guiada, con simulación previa y verificación
Evidencia	Capturas y planillas armadas a última hora	Bitácora inalterable, exportable para el auditor
Reporte a dirección	Presentaciones hechas a mano	Informe ejecutivo con tendencia de postura

23

familias de sistemas operativos con contenido CIS nativo

70k+

reglas de configuración segura listas para usar

< 5 min

desde la instalación del agente hasta el primer resultado

100%

estándares abiertos, sin dependencia de formatos propietarios

De la detección a la evidencia, en un solo lugar.

Agentes ligeros, evaluación continua, hallazgos priorizados, remediación y trazabilidad: un ciclo cerrado que su equipo opera desde un único panel.



Despliegue en minutos

Un agente ligero para Linux, Windows y macOS que se instala con un solo comando y se mantiene actualizado por sí mismo.



Evaluación continua

Escaneos programados contra CIS Benchmarks. Cualquier desviación de la línea base se identifica de inmediato.



Políticas adaptadas al negocio

Excepciones por entorno con justificación registrada. El auditor ve qué control se ajustó, quién lo aprobó y por qué.



Remediación con control

Cada hallazgo incluye su corrección. Se puede simular antes de aplicar, verificar con un re-escaneo y revertir si es necesario.



Exposición a vulnerabilidades

Inventario de software por equipo y correlación con vulnerabilidades conocidas, junto a la postura de configuración.



Multi-organización

Cada cliente, filial o unidad de negocio opera aislada, con su propio tablero. Ideal para grupos empresariales y MSSP.



Alertas e integraciones

Notificaciones ante degradación de la postura y envío de hallazgos a las herramientas de gestión que su equipo ya utiliza.



Reportes para cada audiencia

Informe ejecutivo para la dirección y detalle técnico para operaciones. Plataforma disponible en español, inglés y portugués.

CÓMO FUNCIONA

1

Incorpore su flota

Instale el agente en servidores y estaciones. Cada equipo queda identificado y en línea.

2

Defina la línea base

Elija el perfil CIS adecuado y ajuste las reglas que no aplican a su entorno.

3

Evalúe sin pausa

Los resultados alimentan el indicador de postura de cada organización.

4

Corrija y demuestre

Cierre hallazgos con verificación y entregue evidencia sin trabajo adicional.

Menos superficie de ataque, auditorías previsibles y un equipo enfocado.

RIESGO

Reduzca la exposición de forma medible

- Indicador único de postura por organización
- Tendencia en el tiempo para el comité de riesgos
- Prioridad por severidad, no por volumen

CUMPLIMIENTO

Llegue a la auditoría con la evidencia hecha

- Trazabilidad de cada cambio y excepción
- Hallazgos mapeados a marcos de control
- Exportación lista para el auditor

EFICIENCIA

Libere horas de su equipo técnico

- Sin recolección manual de evidencias
- Correcciones listas para aplicar
- Un solo panel para toda la flota

MARCOS DE REFERENCIA

CIS Benchmarks

NIST 800-53

ISO/IEC 27001

PCI DSS

DISA STIG

HIPAA

SOC 2

Los resultados técnicos se relacionan con los marcos que su organización debe atender, para que un mismo esfuerzo de hardening sustente varias obligaciones. Las marcas citadas pertenecen a sus respectivos titulares.

SEGURIDAD POR DISEÑO

- ✓ Aislamiento estricto de datos entre organizaciones
- ✓ Cifrado en tránsito y en reposo
- ✓ Autenticación multifactor e inicio de sesión único (SSO)
- ✓ Comunicación autenticada con cada agente
- ✓ Bitácora de auditoría inalterable

Vea su postura real en una sesión de trabajo.

Agende una demostración con su propio entorno de prueba y conozca en minutos el estado de configuración de sus sistemas.

Solicitar demostración

vectoraiq.dev