Claude Security. Setup completo. Actívalo hoy mismo.

CATEGORÍA · SEGURIDAD Y BUENAS PRÁCTICAS

La herramienta que acaba de matar a una industria de seguridad enterprise. Aquí está cómo conectarla a tu repositorio en menos de 10 minutos y qué hacer con los primeros findings.

QUÉ VAS A ENCONTRAR

FICHA DEL RECURSO

Qué es, para qué sirve y cómo se implementa

FUNCIÓN

La herramienta que acaba de matar a una industria de seguridad enterprise. Aquí está cómo conectarla a tu repositorio en menos de 10 minutos y qué hacer con los primeros findings.

PARA QUÉ SIRVE

Eso se evaporó esta semana. Anthropic acaba de lanzar Claude Security en beta pública. Es una herramienta que escanea tu repositorio, lo lee como un security researcher humano, traza el flujo de datos y encuentra vulnerabilidades complejas que las herramientas tradicionales pasan por alto. En vez de buscar patrones predefinidos, razona. Y cada finding pasa por verificación multi-etapa para reducir falsos positivos al mínimo. Esto antes te costaba cinco mil dólares al año pagándole a Snyk. Diez mil por una auditoría puntual con un consultor. Treinta mil al año si tenías un equipo grande con Veracode o Checkmarx. Hoy viene dentro de tu plan de Claude. Y si tu producto es open-source, es comple

DÓNDE APLICARLO

Cubre: Cómo activar Claude Security en tu cuenta; Cómo conectar tu primer repositorio en GitHub; Las 4 vulnerabilidades más comunes que detecta; Cómo interpretar findings y aprobar parches; La oportunidad real para founders LATAM.

CÓMO IMPLEMENTARLO

1. Qué Lo Hace Diferente: Razona como humano.
2. Setup En 4 Pasos: Activa Claude Security en menos de 10 minutos.
3. Qué Detecta · 4 Primeras: Las vulnerabilidades que más matan startups.
4. Qué Detecta · Continuación: Path traversal y SSRF.
5. Cómo Leer Los Findings: Crítico, alto, medio.
6. El Flujo De Parches: Suggest fix. Review. Aprueba.
7. Vs La Industria: Claude Security vs Snyk, Veracode, Checkmarx.

EL ÁNGULO

20 mil millones.

Eso se evaporó esta semana. Anthropic acaba de lanzar Claude Security en beta pública. Es una herramienta que escanea tu repositorio, lo lee como un security researcher humano, traza el flujo de datos y encuentra vulnerabilidades complejas que las herramientas tradicionales pasan por alto. En vez de buscar patrones predefinidos, razona. Y cada finding pasa por verificación multi-etapa para reducir falsos positivos al mínimo. Esto antes te costaba cinco mil dólares al año pagándole a Snyk. Diez mil por una auditoría puntual con un consultor. Treinta mil al año si tenías un equipo grande con Veracode o Checkmarx. Hoy viene dentro de tu plan de Claude. Y si tu producto es open-source, es completamente gratis. $5K/año $30K/año SNYK TIER MEDIO STACK ENTERPRISE ACTUAL

QUÉ LO HACE DIFERENTE

Razona como humano.

Y eso cambia todo. Las herramientas viejas funcionan con reglas y patrones. Si una vulnerabilidad no está en su base de patrones, no la ven. Por eso el 60% de los issues críticos en startups LATAM nunca se detectan hasta que ya es tarde. Claude Security cambia el modelo. Lee tu código entero, entiende cómo interactúan los componentes, traza data flows entre archivos, y razona sobre cada path posible. Cuando encuentra algo, te explica por qué es problema y te genera el parche listo para revisión humana.

EL CONTRASTE

Snyk + tools tradicionales: static analysis con reglas.
alta tasa de falsos positivos.
limitado a vulnerabilidades conocidas.
Claude Security: razonamiento como researcher humano.
multi-stage verification.
encuentra vulnerabilidades complejas
que ninguna regla anticipa.

SETUP EN 4 PASOS

Activa Claude Security en menos de 10 minutos.

Claude Security ya está disponible en research preview para clientes Enterprise y Team. Si tu producto es open-source, puedes aplicar a acceso gratuito expedited en claude.com/contact-sales/security. Una vez aprobado tu acceso, el setup completo toma menos de diez minutos.

LOS 4 PASOS

1. Activa la sección Security en tu sidebar de Claude
2. Conecta tu cuenta de GitHub vía OAuth
3. Selecciona el repositorio que quieres auditar
4. Lanza el primer scan completo (toma 1-3 minutos)

QUÉ DETECTA · 4 PRIMERAS

Las vulnerabilidades que más matan startups.

01 · COMMAND INJECTION

Cuándo aparece: cuando tu código pasa input del usuario directo a una shell. Ejemplo real: un endpoint de webhooks que ejecuta scripts según el payload. Severidad típica: Critical. Lo que el atacante logra: ejecutar
comandos arbitrarios en tu servidor.
02 · JWT AUTHENTICATION BYPASS
Cuándo aparece: cuando tu validación de tokens acepta el algoritmo "none" o no verifica la firma correctamente. Severidad típica: Critical. Lo que el atacante logra: hacerse pasar por cualquier usuario sin contraseña.

QUÉ DETECTA · CONTINUACIÓN

Path traversal y SSRF.

Las que pasan por alto.

03 · PATH TRAVERSAL

Cuándo aparece: cuando tu endpoint de descarga acepta nombres de archivo sin sanitizar. Ejemplo: "../../../etc/passwd" en una URL. Severidad típica: Critical. Lo que el atacante logra: leer archivos sensibles del
servidor.
04 · SERVER-SIDE REQUEST FORGERY (SSRF)
Cuándo aparece: cuando tu servicio hace requests a URLs definidas por el usuario sin validación. Ejemplo: validador de URLs que permite localhost o redes internas. Severidad típica: High. Lo que el atacante logra: acceder a servicios internos detrás del firewall.
Estas 4 son las que más comúnmente aparecen en repos LATAM auditados. Claude Security las detecta con
multi-stage verification, lo que reduce falsos positivos a casi cero.

CÓMO LEER LOS FINDINGS

Crítico, alto, medio.

Y qué hacer con cada uno. Cada finding viene con severidad asignada según impacto y explotabilidad. La regla operativa es simple: arregla lo crítico hoy, lo alto esta semana, lo medio este mes.

PROTOCOLO DE TRIAGE

CRITICAL → arregla en menos de 24 horas
si la app está en producción.
puede causar breach o pérdida total.
HIGH → arregla esta semana.
requiere condiciones específicas
pero es explotable.
MEDIUM → arregla este mes.
reduce superficie de ataque.
LOW → documenta y revisa próximo sprint.

EL FLUJO DE PARCHES

Suggest fix. Review. Aprueba.

Cuando le das click a "Suggest fix" en cualquier finding, Claude Security analiza el problema profundamente, propone un parche específico y te muestra exactamente qué líneas cambiar, en qué archivo, con qué commit. El parche viene con una explicación de por qué resuelve el issue y qué tests recomendados ejecutar antes del merge. Todo queda en tu workflow de Git: el merge sigue siendo decisión humana. La velocidad real de este flujo es lo que mata a la industria entera de seguridad enterprise. Lo que antes era un ciclo de 2-3 semanas (detectar, escalar, contratar consultor, aplicar fix, retestear) ahora es un ciclo de minutos.

REVISIÓN HUMANA OBLIGATORIA

Claude Security NO mergea código solo. Genera el parche, te lo muestra como diff, y espera tu aprobación. La decisión final siempre es del equipo humano.

ERRORES COMUNES

Qué NO hacer con la herramienta.

El error más caro es tratar a Claude Security como un IDE plugin más. No lo es. Es un security researcher virtual que requiere setup mínimo pero criterio humano para operar.

5 ERRORES QUE SE VEN SEGUIDO

1. Aplicar todos los parches sin revisar el diff.
2. Ignorar findings de severidad Medium / Low.
3. Correr scans solo cuando hay un release.
4. No documentar los findings que dismisseaste.
5. Asumir que cubre todo: sigue siendo capa única.

VS LA INDUSTRIA

Claude Security vs Snyk, Veracode, Checkmarx.

La diferencia no está solo en el precio. Está en el modelo. Y eso es lo que hace que esta sea una transferencia de mercado, no una competencia más.

TABLA COMPARATIVA

	Snyk/Veracode	Claude Security
Costo anual	5K - 30K USD	incluido en plan
Modelo	static analysis	reasoning
Falsos positivos	altos	bajos
Genera parches	no	sí
Open-source	pago	gratis
Setup	complejo	4 pasos

LA JUGADA

Por qué esto te da ventaja.

Si construyes en LATAM, esta noticia te toca distinto que a un founder de Silicon Valley. La mayoría de startups LATAM no podía pagar seguridad enterprise. Eso es por qué el 60% de las vulnerabilidades nunca se detectan: no hay budget para detectarlas. Claude Security baja el costo a casi cero. Significa que tu startup puede tener nivel de seguridad de empresa Fortune 500 desde el día 1. Eso desbloquea ventas a clientes enterprise que antes te decían no por compliance. construir SaaS V2 en LATAM con infraestructura de primer mundo a precio de ground zero.

PRIMER MOVIMIENTO

1. Activa Claude Security esta semana.
2. Corre el primer scan en tu repo principal.
3. Documenta todos los findings críticos.
4. Usa esto como argumento de ventas en tu próxima propuesta a cliente enterprise.

CHECKLIST DE PUESTA EN MARCHA

Lo que tienes que hacer esta semana.

HOY MISMO

Aplicar a Claude Security (Enterprise/Team o open-source)
Confirmar acceso aprobado en tu cuenta de Claude
Conectar GitHub vía OAuth
ESTA SEMANA
Correr primer scan en tu repositorio principal
Documentar findings críticos en /security/audit-[fecha].md
Aplicar parches sugeridos a vulnerabilidades Critical
EL MES QUE VIENE
Configurar scans automáticos en cada PR
Crear protocolo de triage interno por severidad
Cancelar suscripción de Snyk si la tenías activa

SIGUIENTE PASO

Tu repo está listo. Hoy o mañana.

Aplica a Claude Security ahora mismo. El primer scan toma 3 minutos y los findings que encuentres en repos viejos te van a sorprender. Si eres open-source, el acceso es gratis y expedited.

MÁS GUÍAS GRATIS EN 377CREATIVE.COM/RECURSOS