Identity Rules

BRIEF POR ROL

SECURITY ANALYST · SOC E IR ANALYSTS.

Cada alerta con todo el contexto de identidad — sin pivotear entre 5 herramientas.

Pasa de la alerta del SIEM al detalle completo de identidad en un click: cuentas, privilegios, actividad reciente, attack paths. Reduce MTTR sin agregar fricción.

60%[1]	45 : 1[2]	10x[3]
de las brechas empiezan con identidad comprometida	NHI por cada identidad humana	más rápido que IGA tradicional

Fuentes: 1) IDSA 2024. 2) CyberArk 2024. 3) Datos internos de pilotos, 2025.

Lo que pesa en tu día a día

Alertas sin contexto de identidad 01

El SIEM dispara una alerta y tienes que pivotear a 3 herramientas para entender quién es la identidad y qué puede tocar. Identity Rules entrega el contexto inline.

MTTR alto en incidentes de identidad 02

Investigar manualmente cada cuenta toma horas. Línea de tiempo automática, mapa de privilegios y attack paths reducen el tiempo a minutos.

Alert fatigue 03

Demasiadas alertas, poco contexto. Detección con IA de patrones reales reduce falsos positivos.

Pivot rápido durante triage 04

Asistente IA conversacional — pregunta en lenguaje natural, recibe respuestas con evidencia. Sin escribir SQL ni KQL.

Identity Rules

BRIEF POR ROL

• RESULTADOS

Cómo Identity Rules te apoya

✓

MTTR reducido drásticamente

Investigaciones que tomaban horas se cierran en minutos con contexto completo.

✓

Triage con menos fricción

El analista resuelve sin pivotear entre 5 consolas.

✓

Menos alertas falsas

Modelos que aprenden el patrón normal y solo elevan lo que importa.

• POR QUÉ IDENTITY RULES

01

Speed to Value

Despliegue hasta 10x más rápido. Sin proyectos largos de IGA, sin meses de integración, sin stack de infraestructura nuevo.

02

Menor costo y complejidad

Reduce el TCO eliminando la sobrecarga operativa de las IGA tradicionales. Modelo SaaS o on-prem con mismo motor.

03

Identity Intelligence con IA

Convierte datos de identidad en insights accionables. Acelera la detección, investigación y respuesta con un copiloto conversacional.

04

Listo para el SOC

Contexto inmediato sobre identidades, cuentas y privilegios para acelerar la detección y respuesta a incidentes.

COBERTURA NHI

45 : 1 [2]

Las NHI ya superan 45 a 1 a las humanas — y son donde nacen los ataques modernos.

Cuentas de servicio
AD, Linux, BD, aplicaciones — quién las creó y quién las usa hoy.

API keys y tokens
Inventario, owner, último uso y rotación.

Bots y CI/CD
Pipelines, automatizaciones y scripts con credenciales.

Workload identities
Roles IAM en AWS/Azure/GCP, service accounts en Kubernetes.

Agentes de IA
Anthropic, OpenAI y otros LLM — qué pueden tocar y con qué privilegios.

Aplicaciones OAuth
Apps de terceros con acceso delegado a tus tenants.

CUANDO QUIERAS CONVERSAR

Agenda 30 minutos con el equipo

idrules.ai/roles/security-analyst

Guillermo Cataneo
Fundador & CEO
guillermo@idrules.ai
linkedin.com/company/identityrules