Identity Rules

ROLE BRIEF

SECURITY ANALYST · SOC AND IR ANALYSTS.

Every alert with full identity context — no pivoting across 5 tools.

From a SIEM alert to full identity detail in one click: accounts, privileges, recent activity, attack paths. Cut MTTR without adding friction.

60%[1]	45 : 1[2]	10x[3]
of breaches start with compromised identity	non-human to human identities	faster to deploy than traditional IGA

Sources: 1) IDSA 2024. 2) CyberArk 2024. 3) Internal customer pilot data, 2025.

What weighs on your day-to-day

Alerts without identity context 01

The SIEM fires and you pivot across 3 tools to figure out who the identity is and what it can touch. Identity Rules delivers context inline.

High MTTR on identity incidents 02

Investigating each account manually takes hours. Automatic timelines, privilege maps and attack paths cut it to minutes.

Alert fatigue 03

Too many alerts, too little context. AI-driven detection of real patterns cuts false positives.

Fast pivots during triage 04

Conversational AI assistant — ask in plain language, get answers with evidence. No SQL or KQL.

Identity Rules

ROLE BRIEF

• OUTCOMES

How Identity Rules supports you

✓

MTTR cut dramatically

Investigations that took hours close in minutes with full context.

✓

Less friction during triage

Analyst resolves without pivoting across 5 consoles.

✓

Fewer false alerts

Models that learn the normal pattern and only escalate what matters.

• WHY IDENTITY RULES

01

Speed to Value

Up to 10x faster to deploy. No long IGA projects, no months of integration, no new infrastructure stack.

02

Lower Cost & Complexity

Cuts TCO by avoiding the operational overhead of traditional IGA. Same engine for SaaS or on-prem.

03

AI-Driven Identity Intelligence

Turns identity data into actionable insights. Accelerate detection, investigation and response with a conversational copilot.

04

SOC-Ready

Immediate context on identities, accounts and privileges to speed up incident detection and response.

NHI COVERAGE

45 : 1[2]

NHIs already outnumber humans 45 to 1 — and they're where modern attacks start.

Service accounts
AD, Linux, DB, applications — who created them and who uses them today.

API keys & tokens
Inventory, owner, last used and rotation status.

Bots and CI/CD
Pipelines, automations and scripts that hold credentials.

Workload identities
IAM roles in AWS/Azure/GCP, Kubernetes service accounts.

AI agents
Anthropic, OpenAI and other LLM keys — what they can touch and with which privileges.

OAuth applications
Third-party apps with delegated access to your tenants.

WHENEVER YOU WANT TO TALK

Book 30 minutes with our team

idrules.ai/en/roles/security-analyst

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