Identity Rules

ROLE BRIEF

CISO · CHIEF INFORMATION SECURITY OFFICER.

Turn identity risk into a clear story for your board.

Identity threat detection, continuous audit evidence and metrics that shrink the IAM attack surface month over month. No endless projects.

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

Reporting risk to the board 01

You need clear, comparable metrics that show progress, not just problems. Identity Rules ships CISO- and board-ready dashboards.

Multi-framework compliance 02

SOX, ISO 27001, PCI-DSS, NIST, local mandates. Centralized evidence exportable per framework instead of chasing admins.

Lower identity-breach probability 03

60% of breaches are identity-related. You need to detect excess privilege and compromised accounts before they escalate.

Justify investment 04

Metrics to prove ROI: dormant accounts removed, orphan privileges spotted, MTTR reduced.

Identity Rules

ROLE BRIEF

• OUTCOMES

How Identity Rules supports you

✓

Actionable risk narrative

Executive reports with trends and concrete actions — not laundry lists.

✓

Painless audits

Continuous evidence available when the auditor arrives, not weeks of prep.

✓

Deploy without a project

No months of integration. Measurable result in week one.

• 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/ciso

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