Identity Rules

INDUSTRY BRIEF

TELECOM · TELCOS AND OPERATORS WITH MASSIVE CUSTOMER DATA.

Identity and access at telco scale — without losing visibility.

Operators with thousands of engineers, dozens of legacy and cloud systems, and millions of subscribers. Identity Rules brings order with one consolidated identity model.

ISO 27001 | GDPR | LOCAL TELCO REG.

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.

Typical blind spots in this sector

Subscriber data access 01

Customer service, billing, anti-fraud, technical support. Detect anomalous access patterns to customer PII.

NHI in OSS/BSS and network 02

Network probes, vendor connectors, provisioning scripts. Full inventory with owner and credential rotation.

Privileged engineers 03

NOC operators, DBAs, field engineers with persistent access. Detect dormant accounts coming back to life and unauthorized escalations.

Multi-country compliance 04

GDPR if you operate in the EU, ISO 27001 globally, local mandates per country. Centralized evidence per tenant and per jurisdiction.

Identity Rules

INDUSTRY BRIEF

• OUTCOMES

What improves with Identity Rules

✓

Lower subscriber-data leak risk

Visibility into who touches customer PII and why — with evidence ready.

✓

NHI under control

Full inventory of service accounts in OSS/BSS, with obsolete ones removed.

✓

Detection ahead of IR

Compromised or abusive accounts spotted before they become a public incident.

• 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.

READY TO DIG DEEPER

Book your Identity Risk Assessment

idrules.ai/en/industries/telecom

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