CASE STUDY | ANVILOGIC ON SNOWFLAKE

How a Fortune 100 Telecom Automates Data Onboarding with Anvilogic on Snowflake

A Fortune 100 telecom is building its security data lake on Snowflake. Anvilogic turns the raw feeds landing there into normalized detection sources and runs the company's detections directly on that data.

THE CHALLENGE

Every feed had to be parsed and normalized by hand. The company hired nine data engineers, at about $1M a quarter, and still had 100+ feeds with no detection coverage.

THE OBJECTIVE

- Clear the backlog of data feeds
- Automate parsing, normalization, and ETL
- Reduce reliance on hand-built ETL

HOW THEY DID IT

Anvilogic Onboard

A Blueprint parses and normalizes each raw Snowflake feed, with an analyst approving every step.

Anvilogic Blueprints

The company's teams build their own Blueprints to automate work they did by hand.

Anvilogic Federated Search

Analysts query Snowflake, Splunk, and SentinelOne from one place, without moving the data.

THE RESULTS

$1M

In consulting scope cut

re-purposed to higher-value work

82%

Priority attack techniques covered

up from 63% in January 2026

3× faster

To deploy an emergency detection

15 minutes, down from 45 to 60

> "Anvilogic is central to our SOC strategy. As we diversify our data strategy to include data lakes, Anvilogic lets us continue SOC operations while giving analysts the ability to reach across data repos."
>
> Security Leadership, Fortune 100 Telecom