CUSTOMER CASE STUDY | ANVILOGIC ON DATABRICKS

How SAP Modernized Detection with Anvilogic on Databricks

Over 90% of Fortune 500 companies use SAP solutions, which requires complex cloud architectures operating at massive global scale. With SAP Enterprise Cloud Services managing more than 200,000 virtual machines and data volumes tripling in recent years, SAP's security team had to rethink its SOC workflows.

THE CHALLENGE

High ingestion costs meant only a subset of SAP's security data could be analyzed in real time, and manual detection engineering consumed analyst time, restricting visibility into threats.

THE OBJECTIVE

- Re-architect data pipelines for a decoupled security model
- Migrate telemetry and detections to Databricks
- Implement AI-powered SOC automation

HOW THEY DID IT

SPL-to-SQL migration

Used Anvilogic's AI capabilities to automate SPL-to-SQL translation of existing detections.

AI-assisted engineering

Generates modular detection logic enriched with MITRE metadata and recommends tuning from historical patterns.

Detections on Databricks

Routed high-volume telemetry to Databricks and fully migrated to a Databricks-native detection architecture.

THE RESULTS

60–80%

Less time spent building detections

freeing analysts for investigative work

5–6×

Faster to build and deploy new rules

so new threats get covered sooner

1–2 months

To do a year of detection work

according to SAP's CISO

> "We were early adopters of the unified workflow Anvilogic and Databricks provide and have been able to transform detection engineering outcomes into business enablers recognized at the board level."
>
> **Roland Costea, Chief Information Security Officer, Enterprise Cloud Services, SAP**