ANVILOGIC™

Stronger Detections, Smarter SOC, Lower Costs

AI SOC Reimagined for SIEMs & Data Lakes

Anvilogic helps you scale detection engineering across your stack through AI-powered triage and unified visibility, with or without a SIEM.

Anvilogic was **founded by a group of former Splunkers and hands-on SOC practitioners** who understood the challenges of legacy SIEM architectures in the age of AI and cloud. Together, they built an **AI-native platform that understands your SOC environment** - built for the speed and complexity of modern business.

Bring Your Technologies

<15 min
To Onboard Feeds to Data Lakes

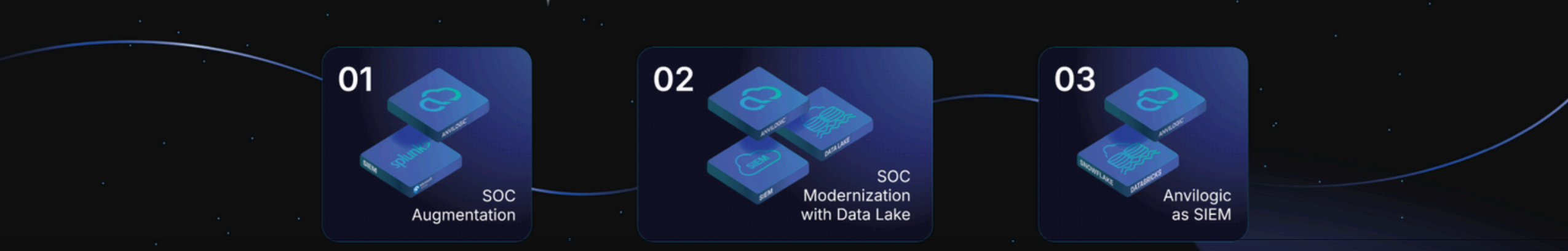
10X
Faster Mean Time to Detect

~80%
More Cost Effective

60%
Reduction in SecOps Manual Tasks

Trusted By the World's Best Brands

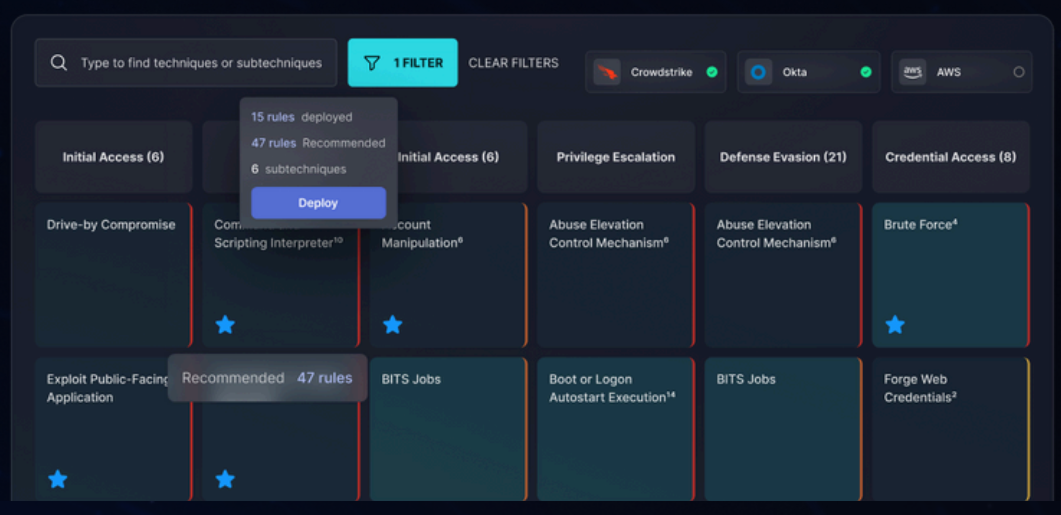
PayPal · sprinklr · Rakuten Mobile · KROLL · REGENERON · SurveyMonkey · Tradeweb · alteryx · First Citizens Bank · crypto.com



Unlike point solutions that handle one step of your program, **Anvilogic's AI SOC powers every workflow - from data onboarding to detection, triage, and investigation - across any lake or SIEM**, giving you the flexibility to change your stack when necessary without sacrificing time or security.

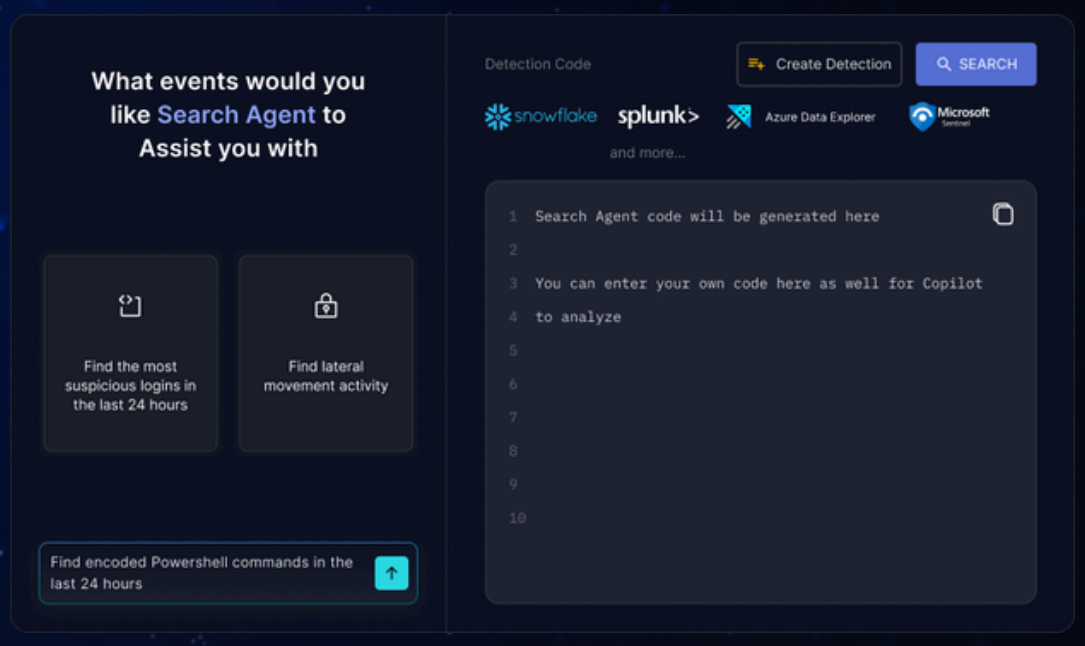
Onboard new data sources in minutes

- Build flexible ETL pipelines that normalize, enrich, and route security data from any cloud storage source (ex. S3, Azure Blob, GCP).
- Remove data silos with streamlined onboarding workflows, ensuring analysts have the complete picture.
- Improve data quality and accessibility, unlocking richer detection and investigation outcomes for not only security teams but other business units.



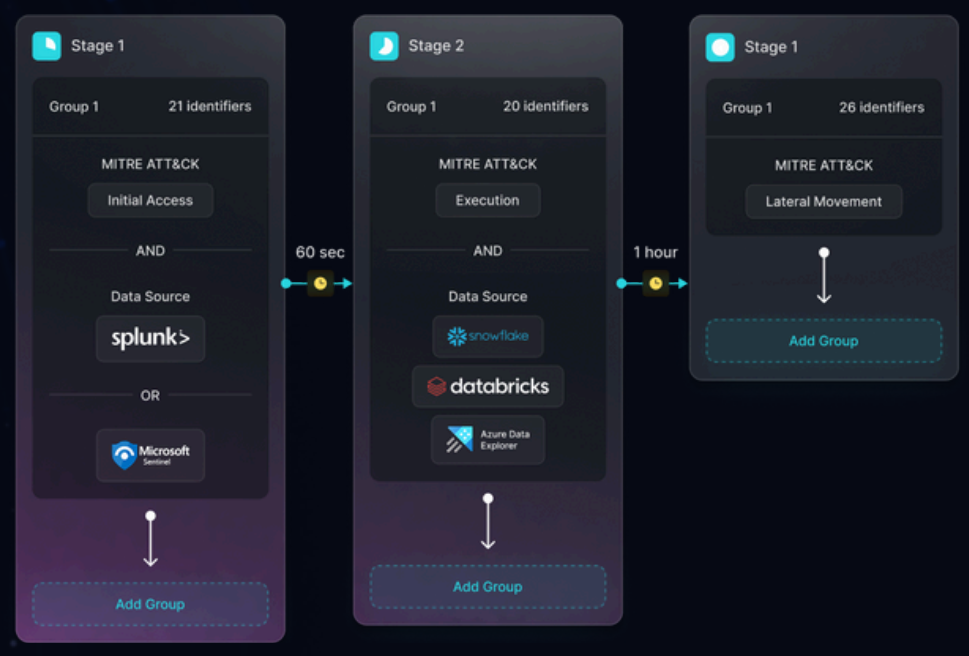
Multi-SIEM & Data Lake Architecture

- Scale analytics cost-effectively by unifying SIEM and data lake environments.
- Eliminate the trade-off between ingesting "all data" vs. "affordable data."
- Centralize threat detection across multiple SIEMs, ensuring consistent coverage regardless of data location.



Rapid, Aligned Correlated Detections

- Build complex correlations in minutes using Anvilogic's modular detection framework.
- Prioritize detections based on MITRE ATT&CK-aligned use cases rather than static rules.
- Reduce noise by surfacing high-fidelity alerts mapped to real adversary behaviors.



AI-Powered SecOps Workflows

- Automate data onboarding, detection engineering, and investigations with AI-driven workflows.
- Empower analysts to move from reactive triage to proactive hunting and response.
- Free up time for strategic security initiatives while reducing manual overhead.

Top 50 in Cybersecurity 2025

Start your AI SOC journey and visit anvilogic.com

ANVILOGIC™