



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



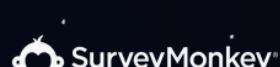
60%

Reduction in SecOps
Manual Tasks

Trusted By the World's Best Brands



REGENERON





Unlike point solutions that handle one step of your program, **Anvilologic'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.



The screenshot displays a dashboard with various threat detection categories and their status. Key elements include:

- A search bar at the top: "Type to find techniques or subtechniques".
- A filter button: "1 FILTER" and a "CLEAR FILTERS" button.
- Logos for CrowdStrike, Okta, and AWS.
- Card-based view of detections:
 - Initial Access (6)**: 15 rules deployed, 47 rules Recommended, 6 subtechniques. Buttons: Deploy, Count.
 - Drive-by Compromise**: Com. Scripting Interpreter¹⁰, Manipulation⁶. Buttons: Deploy, Count.
 - Exploit Public-Facing Application**: Recommended 47 rules. Buttons: Deploy, Count.
 - Privilege Escalation**: Abuse Elevation Control Mechanism⁶.
 - Defense Evasion (21)**: Abuse Elevation Control Mechanism⁶.
 - Credential Access (8)**: Brute Force⁴.
 - Abuse Elevation Control Mechanism⁶**: Buttons: Deploy, Count.
 - Boot or Logon Autostart Execution¹⁴**: BITS Jobs.
 - Forge Web Credentials²**: BITS Jobs.

Multi-SIEM & Data Lake Architecture

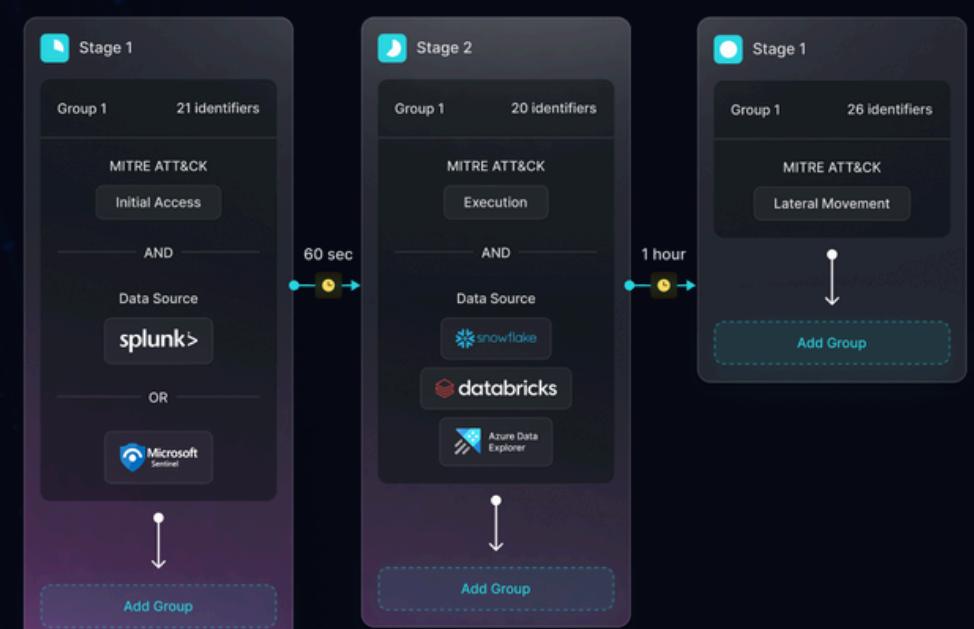
- Scale analytics cost-effectively by unifying SIEM and data lake environments.
- Eliminate the trade-off between ingesting “all data” vs. “affordable data.”
- Centralize threat detection across multiple SIEMs, ensuring consistent coverage regardless of data location.

The screenshot shows a workflow interface with the following sections:

- What events would you like Search Agent to Assist you with?**
- Detection Code**: Buttons for snowflake, splunk>, Azure Data Explorer, Microsoft Sentinel, and more... A note: "Search Agent code will be generated here".
- Find the most suspicious logins in the last 24 hours** and **Find lateral movement activity**.
- Find encoded PowerShell commands in the last 24 hours**.
- Find lateral movement activity** (with a small icon).
- Find the most suspicious logins in the last 24 hours** (with a small icon).

Rapid, Aligned Correlated Detections

- Build complex correlations in minutes using Anvilologic'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.

