ANVILOGIC™

The Next Era Of SIEM: Agentic & Agnostic Flexibility Across Data Stacks

Unify your security data, automate detection engineering & triage workflows, and measure SOC maturity to build an AI SOC

What We Hear

CISOs and CIOs face relentless pressure to:

- Prove ROI on E5 and other tech stack investments
- Cut SIEM costs without sacrificing coverage
- Modernize security without breaking what works
- Future-proof their architecture and plan for life after Splunk

Anvilogic delivers a unified detection & triage platform that:

- Maximizes ROI on E5 and existing SIEMs
- Strengthens coverage across MITRE ATT&CK tactics
- Reduces risk with AI-driven automation and correlation

Strategic Value for Leadership

- Maximize Investments → $1M+ saved annually through automation and cost optimization.
- No Rip-and-Replace → Build on existing tools; avoid the cost, disruption, and risk of major migrations. 90%+ cost savings from data lake diversification.
- Exit Strategy with Control → Transition off a platform safely when you're ready, without breaking visibility or workflows. Out-of-the-box detections, cross-platform correlation.
- Faster Time-to-Value → Noise reduced 43%+ and MTTD cut by 50%+ with agentic triage and continuous measurement of maturity. 40–60% MITRE ATT&CK coverage gains across enterprises.

Supported Data Platforms

Splunk
Augment Splunk with a security data lake

Snowflake
Adopt a data lake alongside your SIEM

Microsoft Sentinel
Transform Sentinel into a detection powerhouse

Databricks
Use more data with a cost effective lakehouse

SOC Augmentation: Automate & Scale Detection Engineering & Alert Triage (Learn More)

- Deploy **thousands of pre-built detections** mapped to MITRE ATT&CK in minutes.
- **Easily build and customize detections** with an intuitive interface; no complex query writing required.
- **AI-powered tuning** insights reduce false positives and manual maintenance.
- **Flexible threat scenario creation** enables teams to design detection logic that fits their unique security needs.
- Threat Scenarios **correlate atomic detections** to prioritize real threats.
- Maturity Scoring continuously **measures and improves detection coverage.**

SIEM Modernization: Detection & Investigation across Multiple Repositories (Learn More)

- Detect threats across **Splunk, Sentinel, Snowflake, Databricks, Azure Data Explorer** and more....no vendor lock-in.
- **Centralized investigation enables** seamless cross-platform correlation.
- Query multiple data sources **without duplicating logs or increasing SIEM costs.**
- **Scale detection** without replacing existing SIEM investments.

Trusted By the World's Best Brands

PayPal · sprinklr · Rakuten Mobile · ebay · REGENERON

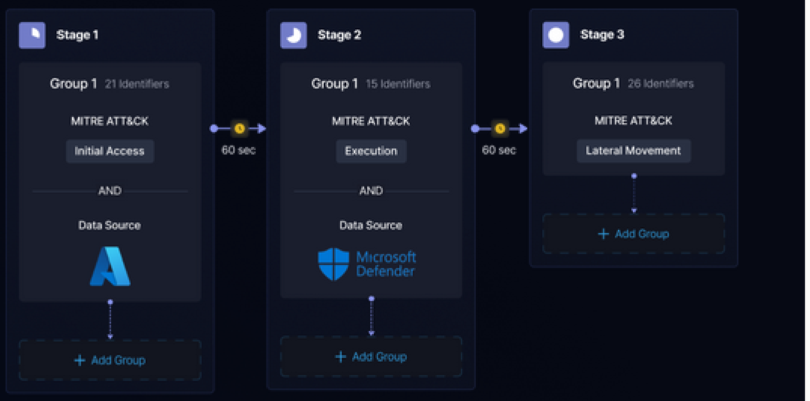
SurveyMonkey · Tradeweb · alteryx · First Citizens Bank · crypto.com

Learn more: anvilogic.com

ANVILOGIC™

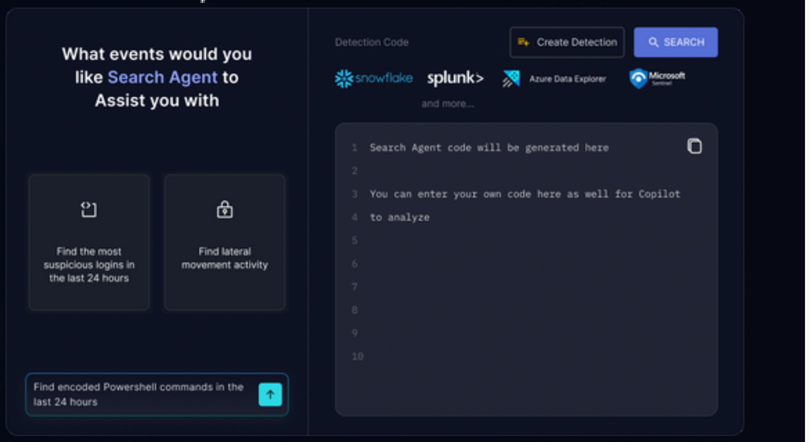
The Armory: Pre-Built Detections & Threat Scenarios

- **Threat Identifiers –** Single-stage, atomic detections mapped to **MITRE techniques.**
- **Threat Scenarios –** Correlate multiple detections for **higher-fidelity alerts.**
- **Detection Gap Analysis –** AI-driven recommendations to fill MITRE coverage gaps.
- **Macros –** Normalize raw logs for **consistent detection across platforms.**
- **Personalized Workspace –** Modify, customize, and deploy detections instantly.



Agentic Workbench & SOC Workflows

- **Build Agent –** Generate SPL, KQL, and SQL detection logic in natural language or from threat reports.
- **Tuning Agent –** Validate and analyze detections for tuning opportunities pre- and post-deployment.
- **Search Agent–** AI-driven search across any data platform. Analyze, drill down, and ask follow-up questions directly in chat.


What events would you like Search Agent to Assist you with

Find the most suspicious logins in the last 24 hours

Find lateral movement activity

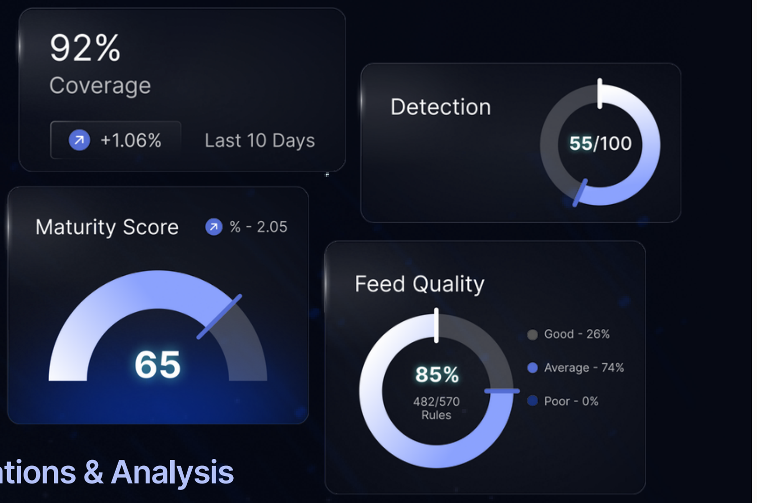
Find encoded Powershell commands in the last 24 hours

```
Search Agent code will be generated here

You can enter your own code here as well for Copilot
to analyze
```

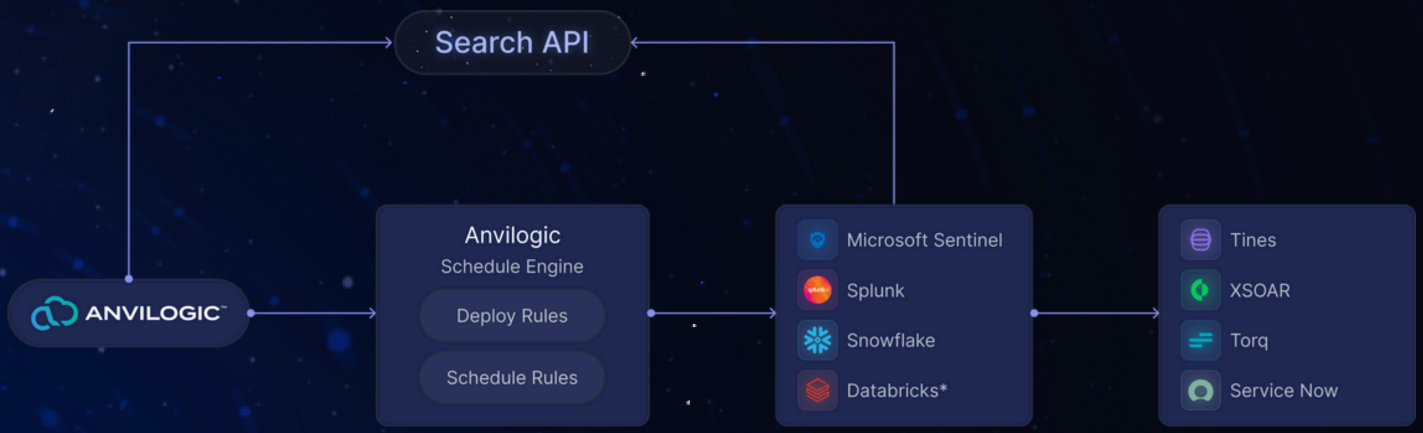
Measure Progress with Maturity Scoring

- **Track & Improve MITRE Coverage –** Identify and prioritize detection gaps based on your environment.
- **SOC Benchmarking –** Compare detection posture over time and against industry peers.
- **Automated Reporting –** Demonstrate progress to leadership with AI-driven insights.



Enhance SOC Workflows with AI Powered Investigations & Analysis

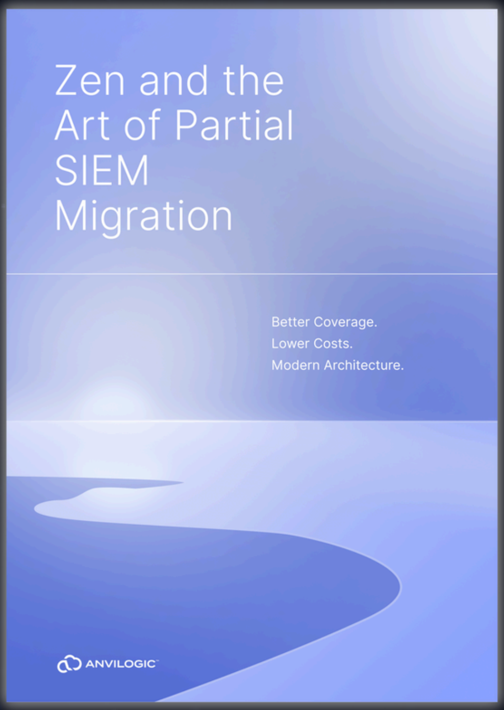
- **Tuning Insights –** Automate noise reduction and detection optimization.
- **Hunting Insights –** Identify hidden threats with AI-assisted escalation.
- **Health Insights –** Ensure detection rules are functioning correctly.
- **Alert Narratives & Dashboards →** Builds multi-chained entity views with reasoning, explanations, and AI assistants guiding enrichment, investigation, and threat hunting with clarity and context.



You Don't Have to Replace Your SIEM Overnight

When people hear "SIEM migration," they imagine a high-stakes overhaul: multi-year projects, full platform shifts, and a scramble to rewire detections from the ground up. **That narrative's outdated.**

Partial SIEM migration is becoming the smarter path forward. Not as a stopgap, but as a strategy.


Zen and the Art of Partial SIEM Migration

Better Coverage.
Lower Costs.
Modern Architecture.

Read Now »

Stronger Detections, Smarter SOC, Lower Costs

Visit anvilogic.com to learn more.

Before Anvilogic, we had no visibility into our detection coverage. The ability to break it down by industry verticals, such as attackers and adversaries, is valuable. Detection insights help us easily identify the most noisy ones, the effective ones, and what needs to be fixed to move the noisy ones to effective ones.

Ajish John
Head of Infosec
SurveyMonkey

Anvilogic is the perfect solution because it doesn't depend on any specific underlying data lake or SIEM solution. It isolates and abstracts the layer of data storage down to the schema, so we don't have to worry about making a big decision for the underlying storage solution. Instead, we have the flexibility to plan for the future.

Guang Wang
Senior Director of Security Operations and Engineering
alteryx

By using a detection engineering platform on top of our data lake, we are able to achieve some significant efficiencies in our overall SOC and IR operations, which can equate to **cost savings of close to 70–80%.**

Prabhath Karanth
Global Head of Security & Trust
NAVAN

By leveraging Anvilogic's support for Azure Data Explorer, the team could efficiently store and query data, choosing it over Microsoft Sentinel for detection engineering. With advanced detection engineering capabilities, pre-built Microsoft detections, and integration with MITRE ATT&CK, Anvilogic helped the team achieve a 30% increase in coverage, significant risk reduction, and cost savings.

Fortune 500 Investment FIrm

With Anvilogic, we now have a technology force-multiplier. It helps us do more with less, so we're less reliant on the number of staff. It allows us to reduce the time it takes to onboard logs and create detections. As a result, we can create more detections with increased complexity, which helps with our overall coverage.

Tim Yip
Global Head of Cyber Security Services
crypto.com

ANVILOGIC™