ANVILOGIC SOLUTION GUIDE

# Modernize Your Security Operations with Automated Threat Detection, Hunting, Triage & Response

Bring together your people, process, technology, and governance to better reduce risk and cost while helping to accelerate business growth through a AI-driven SOC Platform for threat detection and incident response (TDIR).

Even with all the security tools, the data silos and manual detection make it hard to identify high-fidelity threats in your unique environment. While needing to correlate across your hybrid, multi-cloud, and data lake workload alerts can make it even harder to design detection use cases that identify & resolve these threats in short time frames.

### People

Security teams cannot grow at the speed of the business, nor can they grow to keep up with the threat landscape. Teams need a platform that empowers them to effectively focus on higher fidelity tasks.

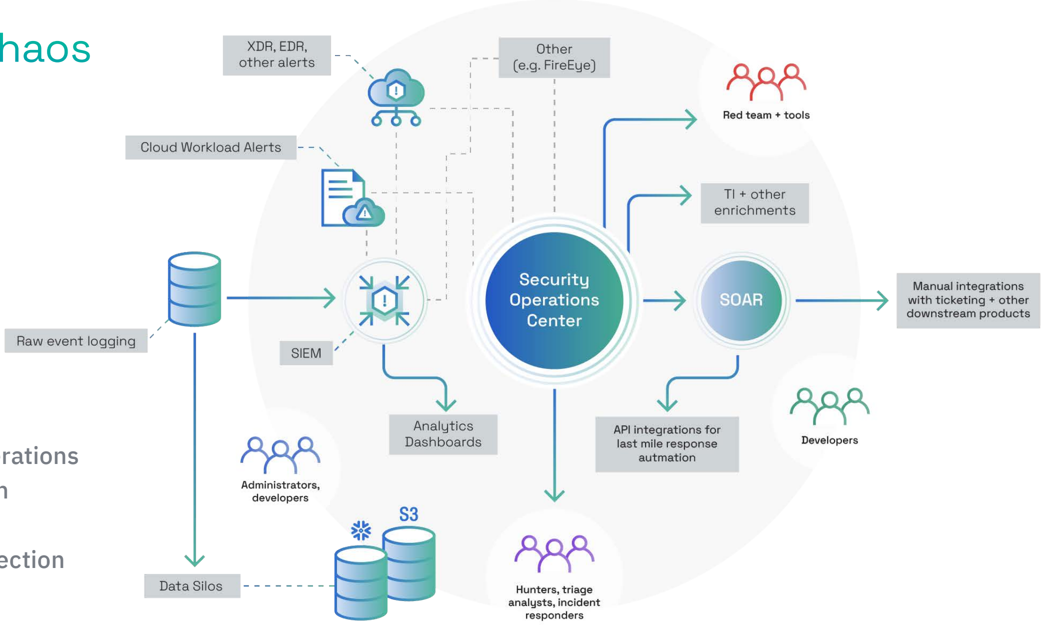
### Process

SOC processes are disjointed today. Effectively building, managing, or implementing automation in SOCs can prove challenging when priorities constantly change and with no clear understanding of one's security posture.

### Technology

SOCs are left with legacy solutions that leave large gaps, manual processes, or expensive services that comprise the bulk of security operations. A platform that connects and automates the SOC lifecycle is needed.

## Today's Security Chaos



- Too many manual human operations
- No holistic AI or collaboration
- Too many disjointed tools
- No correlated "story" for detection & resolution

www.anvilogic.com

ANVILOGIC SOLUTION GUIDE

## What Does It Take To Improve Flexibility & Security Operations In The SOC?

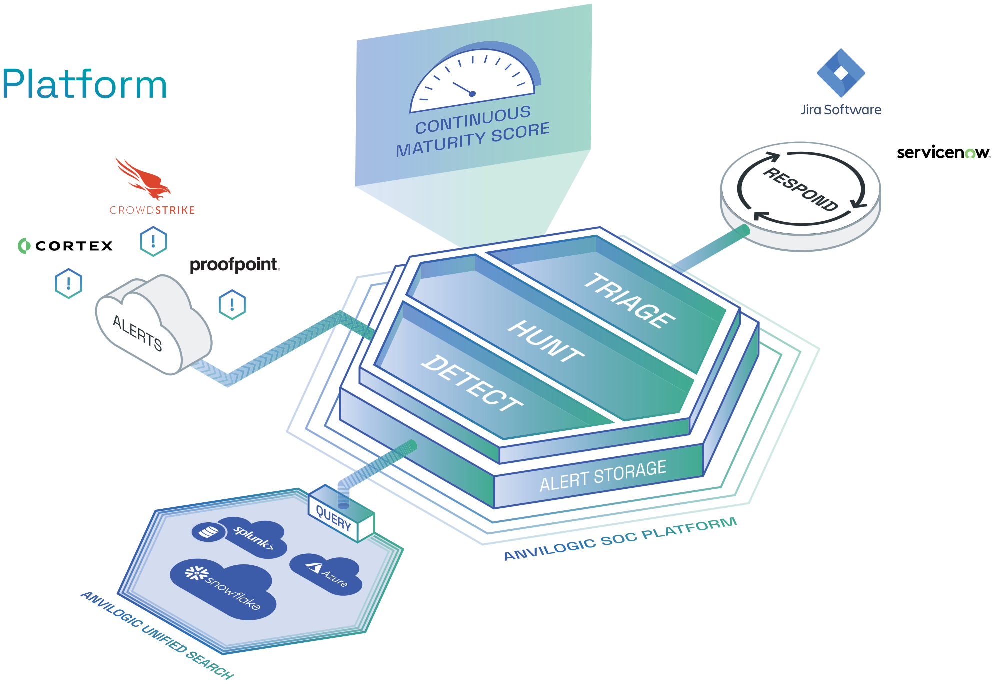
A SOC platform focused on threat detection and incident response can help unify and connect data, processes, and people in a single, harmonious system, enabling you to not choose between security efficacy and or the business. Easily gain business continuity across your security operations, confidently plan, continuously monitor progress and maturity, quickly implement detections with an AI-driven approach for unique environments, and effectively hunt and triage in an integrated workflow.

# A New Hope for the SOC: Move Away From Legacy Solutions

## The ANVILOGIC™ SOC Platform

**Easily correlate across traditional & cloud workloads.**

Consolidate disparate workflow silos, signals, and alerts to better search and across hybrid, multi-cloud and data lakes to better detect produce insights in order to direct the frameworks to ask and answer the right questions specific to your SOC needs.



With automated threat detection and incident response, it's easy for security teams to detect quickly, and effectively hunt and triage the enriched outcomes in a smooth, integrated workflow.

### Better Threat Detection Coverage Visibility

Quickly identify coverage and data gaps through continuous maturity scoring and navigation with ML-Driven recommendations mapped to the MITRE ATT&CK framework.

### Enhance Your Hunting Practices

Hunt for known and unknown patterns. Augment your detections with automated, ML-Driven hunting to find suspicious behavioral attack-patterns and quickly deploy related detections.

### Improved Detection and Response

Reduce time to build pattern-based detections with no-code or deploy out-of-the-box behavioral threat detection content based on frameworks, like MITRE ATT&CK or customized kill chains.

### Automate alert collection & normalization

Automatically ingest, normalize, tag, and enriched signal from tools before events are indexed. One-step integration of your ServiceNow, Jira ticketing and case management systems for immediate response.

ANVILOGIC™
www.anvilogic.com