Advanced Threat Detection: The Anvilogic Approach

Coverage with Confidence. Hunt with Intention.

Finally...A Hunting Co-Pilot

Take the guesswork out of advanced threat detection and start hunting now. Let ML do the grunt work and leverage Purple Team-tested detections.

Anvilogic's approach to Advanced Threat Detection (ATD) automates the human approach of hypothesis-driven hunting while leveraging machine learning (ML) to provide you with actionable insights. Weave the story of an incident together with intention — not guesswork — by utilizing Anvilogic's ATD to bring efficiency and assurance to hunting and finding hidden threats.

Bolster Your Hunting Resources

An augmented hunting experience to nurture and enable analysts with automated ML-driven analysis of suspicious activities and patterns

Out-of-the-Box, But No Black Box

A starting point for your SOC with over 1,000 high-quality detections that are easy to deploy, customize, and manage

Trends at Your Fingertips

Trending threats from across the globe keep you informed of what may impact your business and the detections to find them

Navigate Through Your Data

Prescriptive guidance throughout the detect, hunt, triage, and response lifecycle with ML-based recommendations

"The Armory is awesome - it's like a search engine for detections. When we want to try detecting something, we first look at The Armory before trying to create one on our own. Then, if it's already in there, we deploy it."

– Jason Murphy

Director of Information Security

St. George's University

ATD Features

The Armory

Force multiply and increase productivity by leveraging our purple team researchers with over 60 years of collective cybersecurity experience to provide your team with battle-tested content

- A growing collection of ready-to-deploy detection rules that are easy to customize and maintain
- Trending topics surfaces newsworthy threats, vulnerabilities, and campaigns that may impact your environment with the recommended logic to find them
- Expert generated threat research and intelligence at your fingertips

Anvilogic Hunting Framework

Bolster your hunting resources by using our Hunting Framework to automatically identify, elevate, and escalate advanced threats within your environment

- Escalates suspicious activity with ML-driven recommendations to take action
- Sends significant alerts to triage for investigation
- Enriches data to find and remove false positives or unwanted alerts

Targeted Machine Learning

Let the machines do the work alongside you by leveraging prescriptive guidance and recommendations from threat hunter-trained ML

- Augments your existing hunting resources by highlighting suspicious behavior that you may (or may not) have a detection for
- ML finds and escalates suspicious patterns in your Events of Interest (or high-fidelity alerts) — not your raw data — so you don't miss a thing
- Benefit from ML models that learn from real threats across your peer group

Broader Platform Benefits

Go from threat to detect in minutes by streamlining and unifying your threat detection processes across your hybrid logging platforms

- The Anvilogic platform search and queries data from your distributed environment
- Leave your data where you want it and connect through API
- Quickly build an attack story based on your unique environment using a no-code scenario builder that maps to the MITRE ATT&CK framework

Customer Spotlights

Anvilogic helped **St. George's University** roll out detections 3x faster than their SIEM.

Within one week, Anvilogic helped a **Fortune 500 Financial Services Company** detect two red team attack simulations.