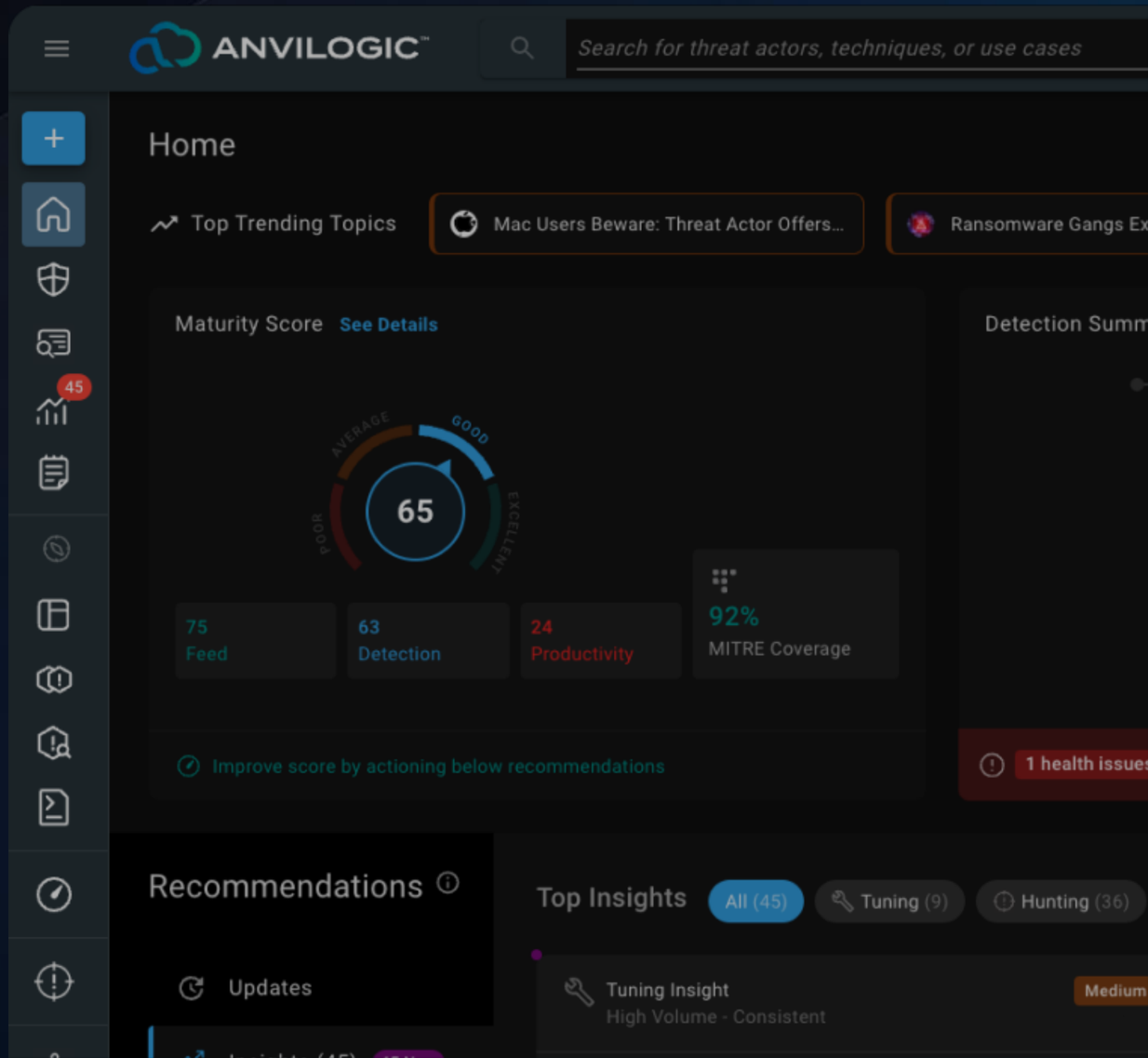
ANVILOGIC™

Anvilogic

Helping leading security teams to mature & streamline their detection engineering

What to Expect:

- 6 Visuals
- Architecture
- Interactive Demo



ANVILOGIC™

PM & Podcast Host

All Things Detection Engineering

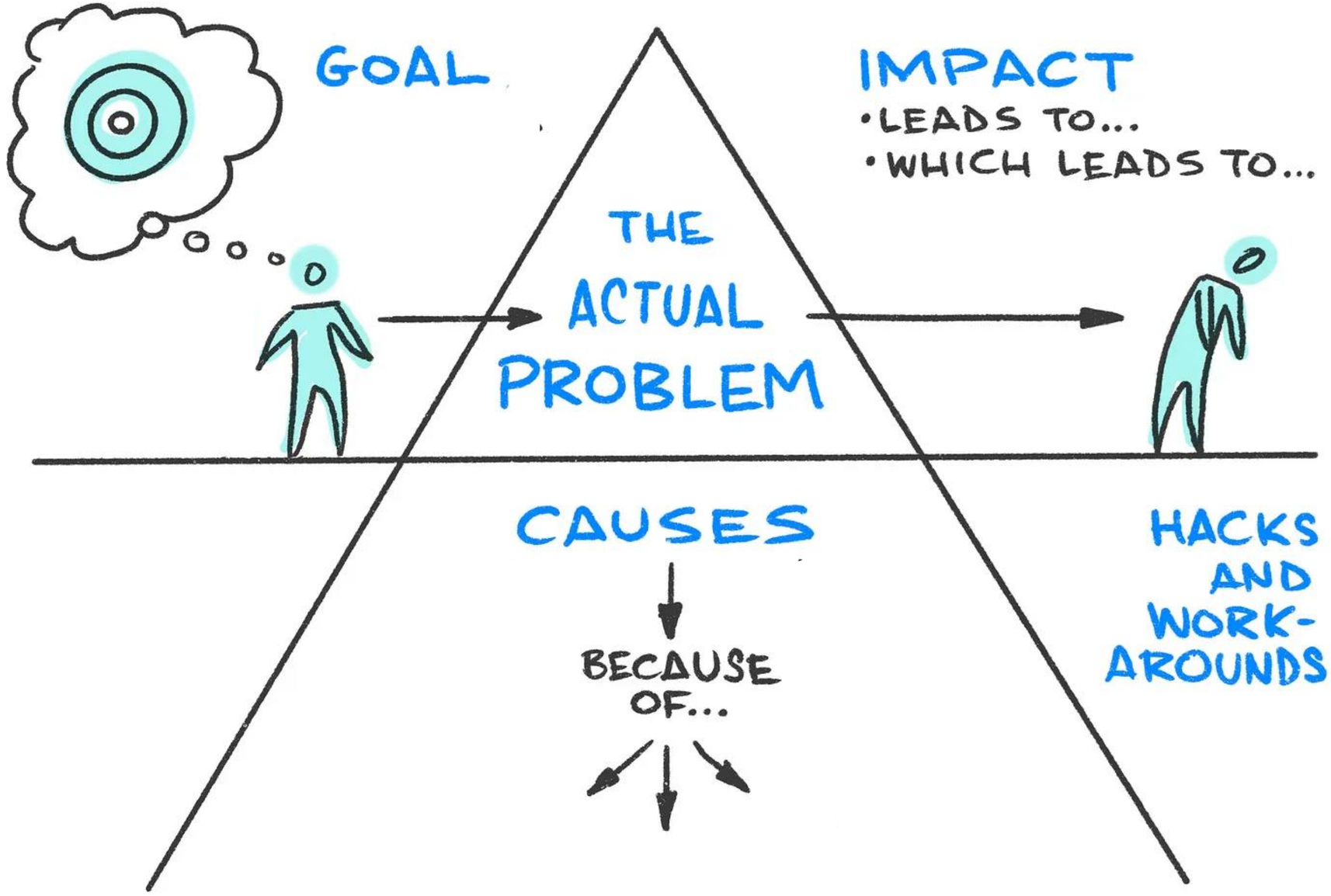
Every Other Thursday | Live via Zoom

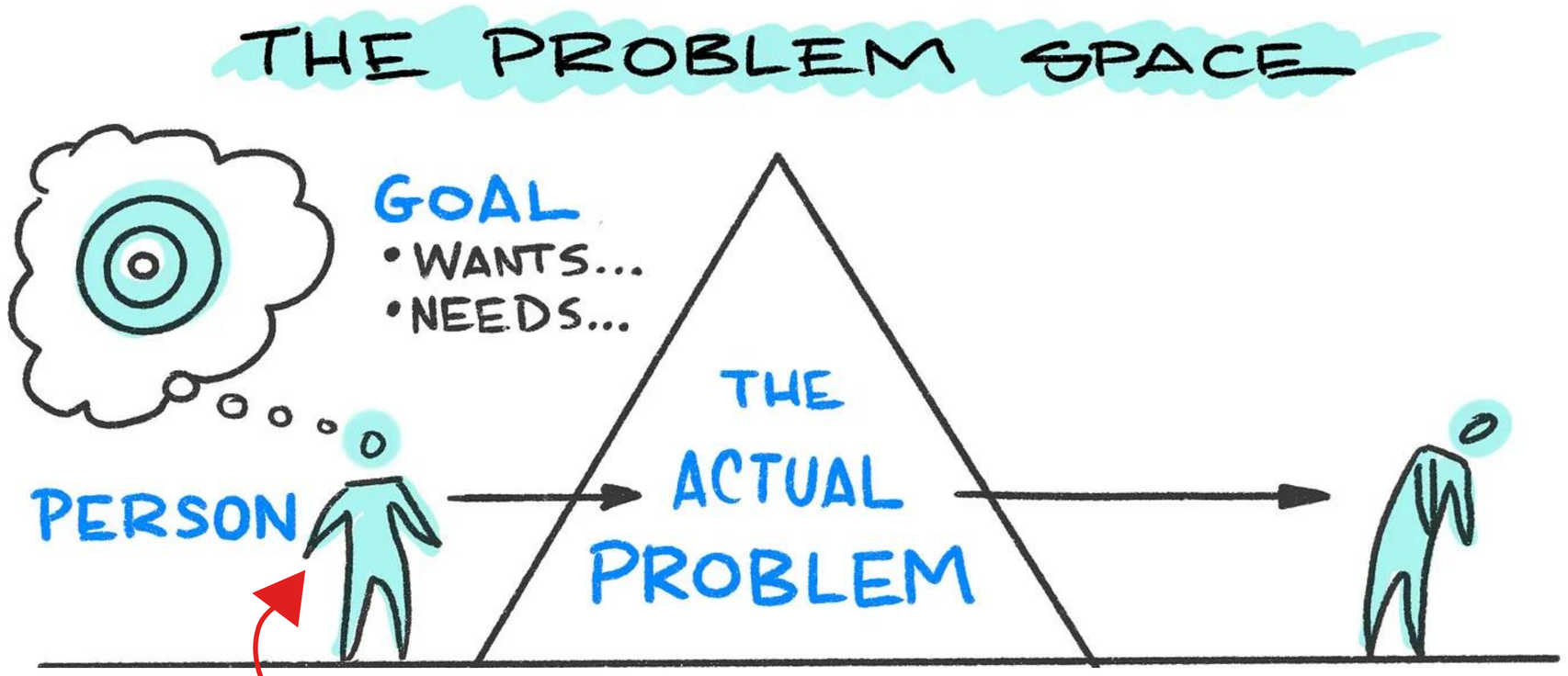
DETECTION ENGINEERING DISPATCH

Join the Community

CYBER SOLUTIONS FEST 2024

THE PROBLEM SPACE





Detection Engineer
Build Detections
or Tuning your peers detections
Threat Research
Operationalize TTPs
Threat Modeling
Report on ^^

1. **Tedious AF**
2.

Detection Engineering is critical but is slow and manual

Creating Detections is Slow

> 1 week

to create and deploy new detections in their environment (84% surveyed)

Manual Maintenance

3 FTEs

Correspondents surveyed say at least 3 people yearly required to tune & validate detections yearly.

Limited Progress

67%

Feel they haven't made significant improvement on detection maturity from previous year.

The Data Problem

75%

Feel they do not have access to all the logging required to meet detection objectives

Detection Engineering and Hunting are Critical

60%

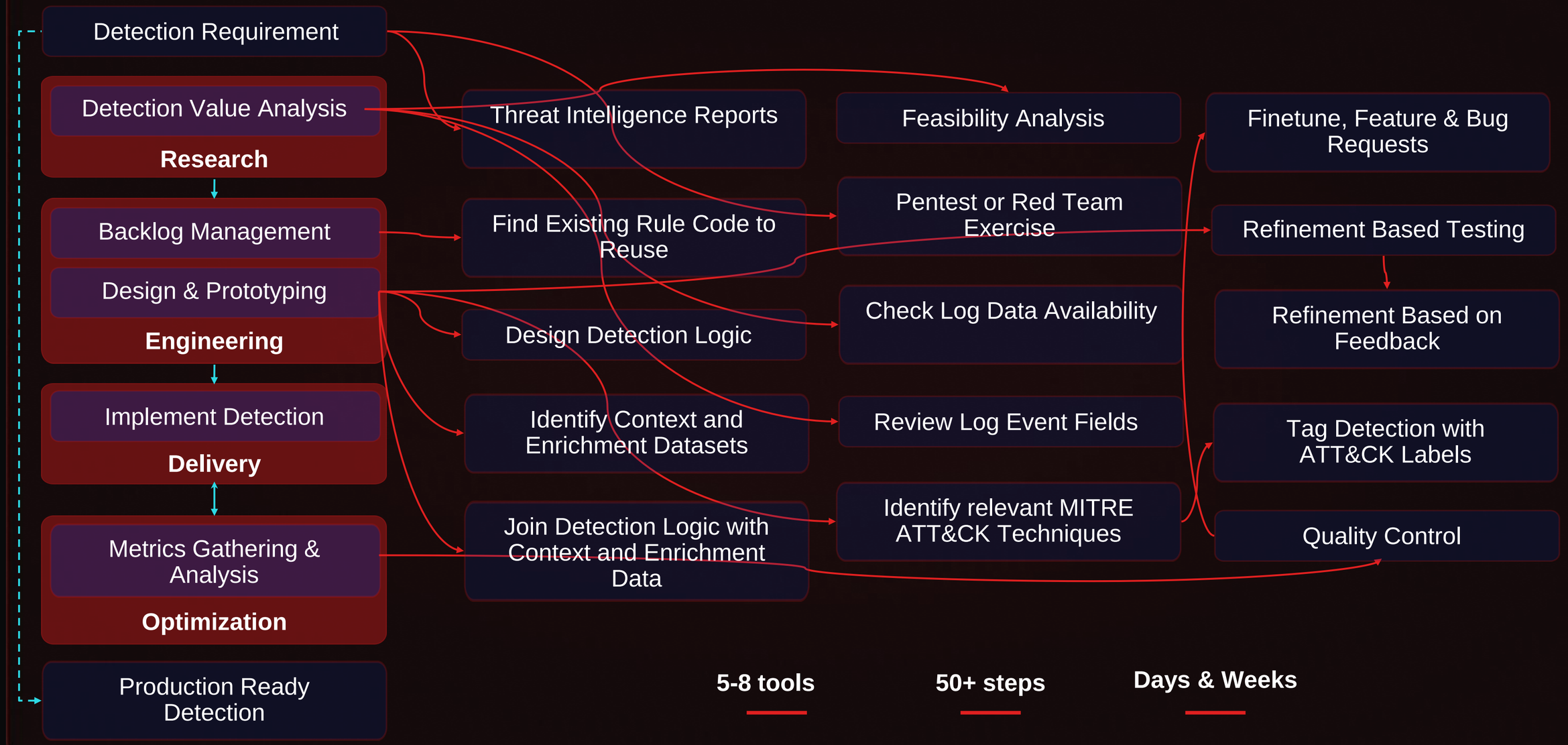
of the security professionals surveyed, feel that time spent on detection engineering is **more valuable than nearly any other activity** that time could be used on.

Sources:
ESG
Anvilogic POCs

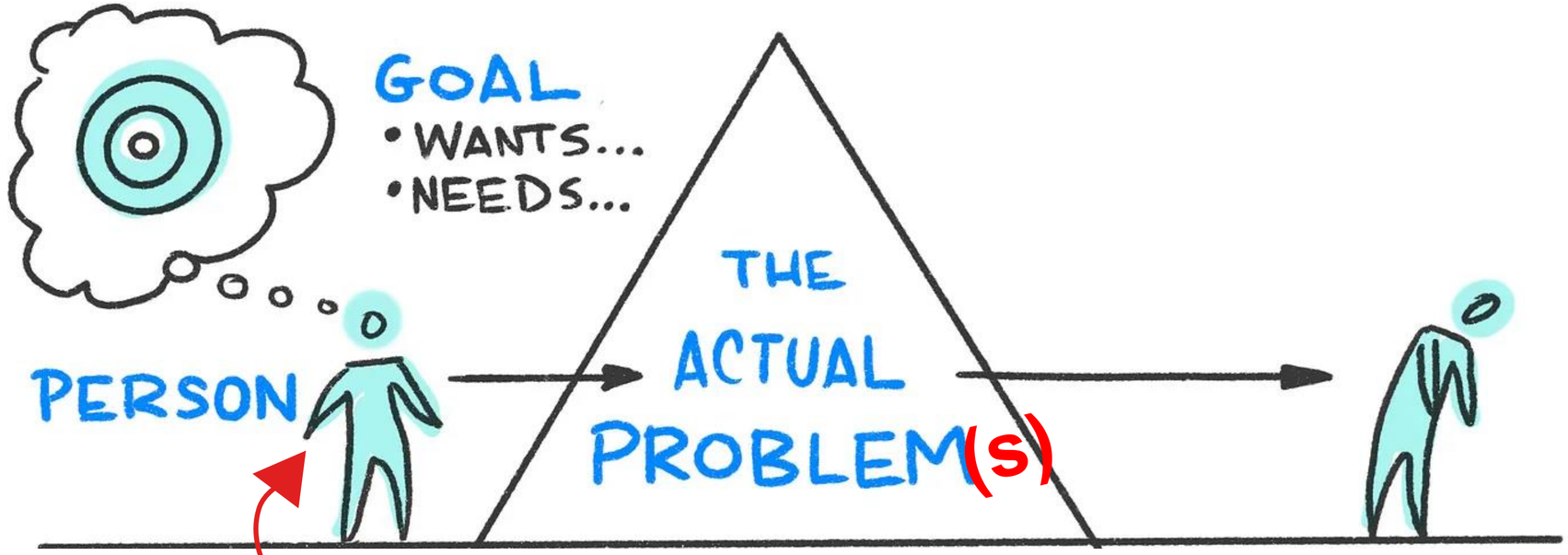
ANVILOGIC™

To Go from Threat to Detection Today

Detection Engineer's Typical Workflow Complexity



THE PROBLEM SPACE

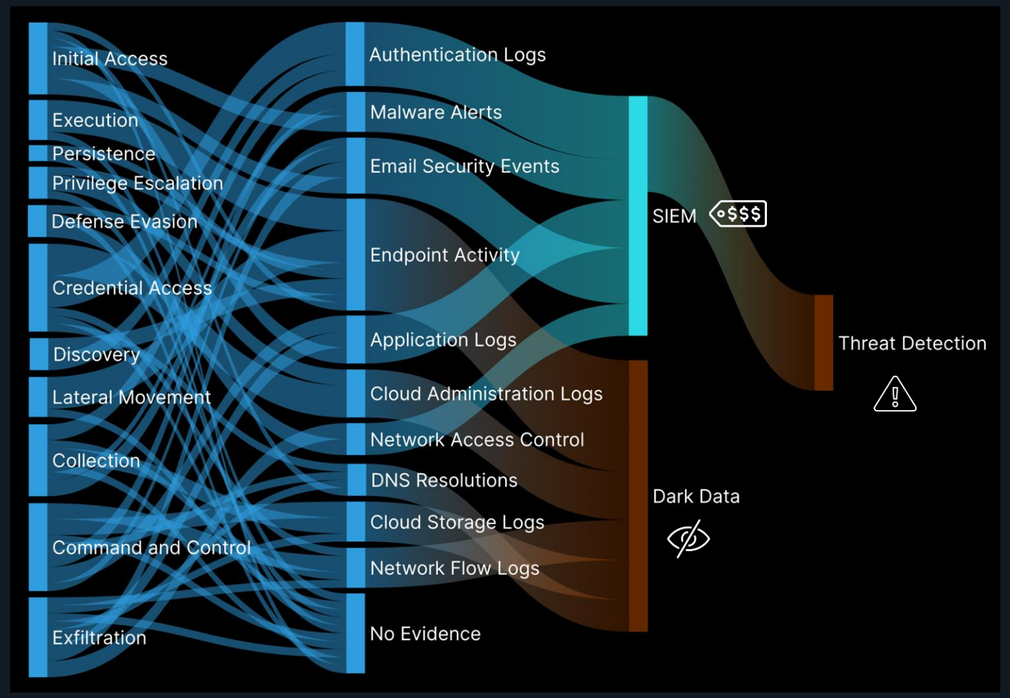


Detection Engineer
Build Detections
or Tuning your peers detections
Threat Research
Operationalize TTPs
Threat Modeling
Report on ^^

1. **Tedious AF**
2. **SIEM Lock-in**

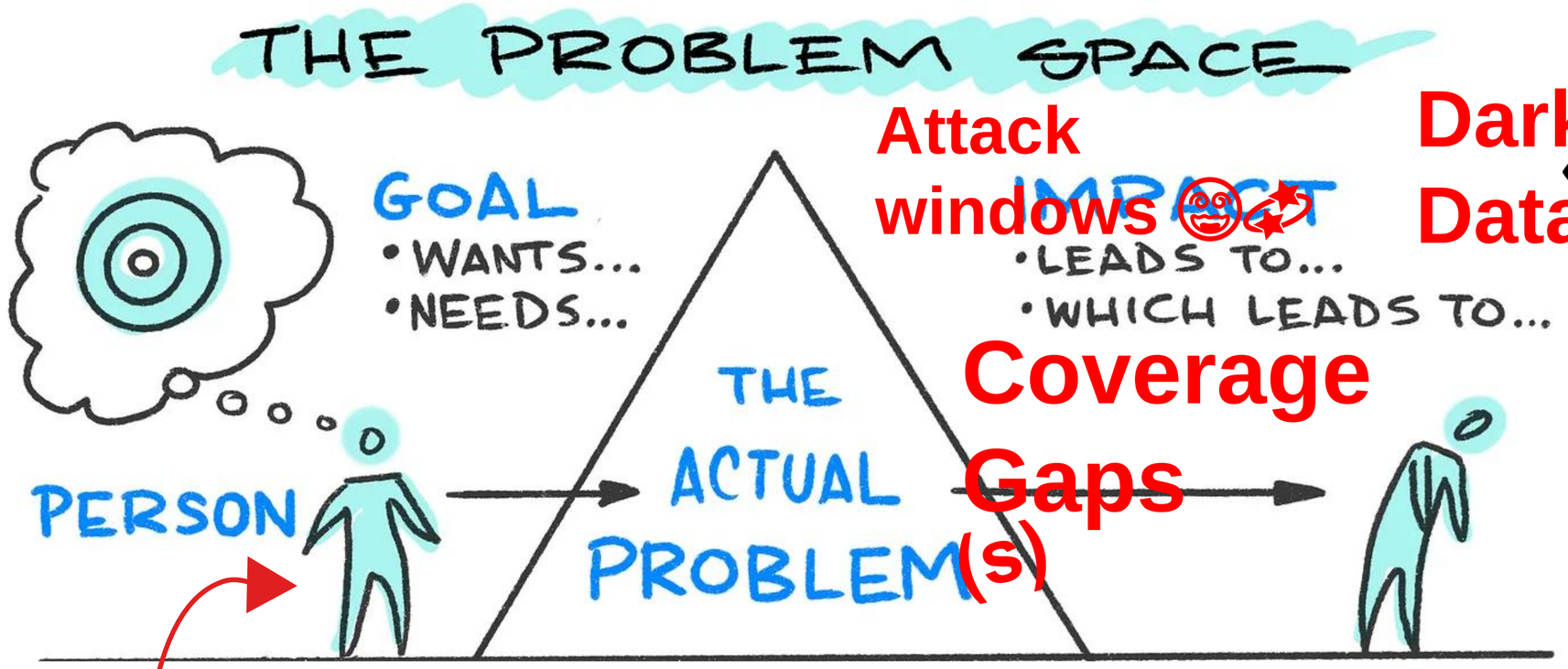
SIEM Lock-in Holds Us Back

Dark data creates detection gaps



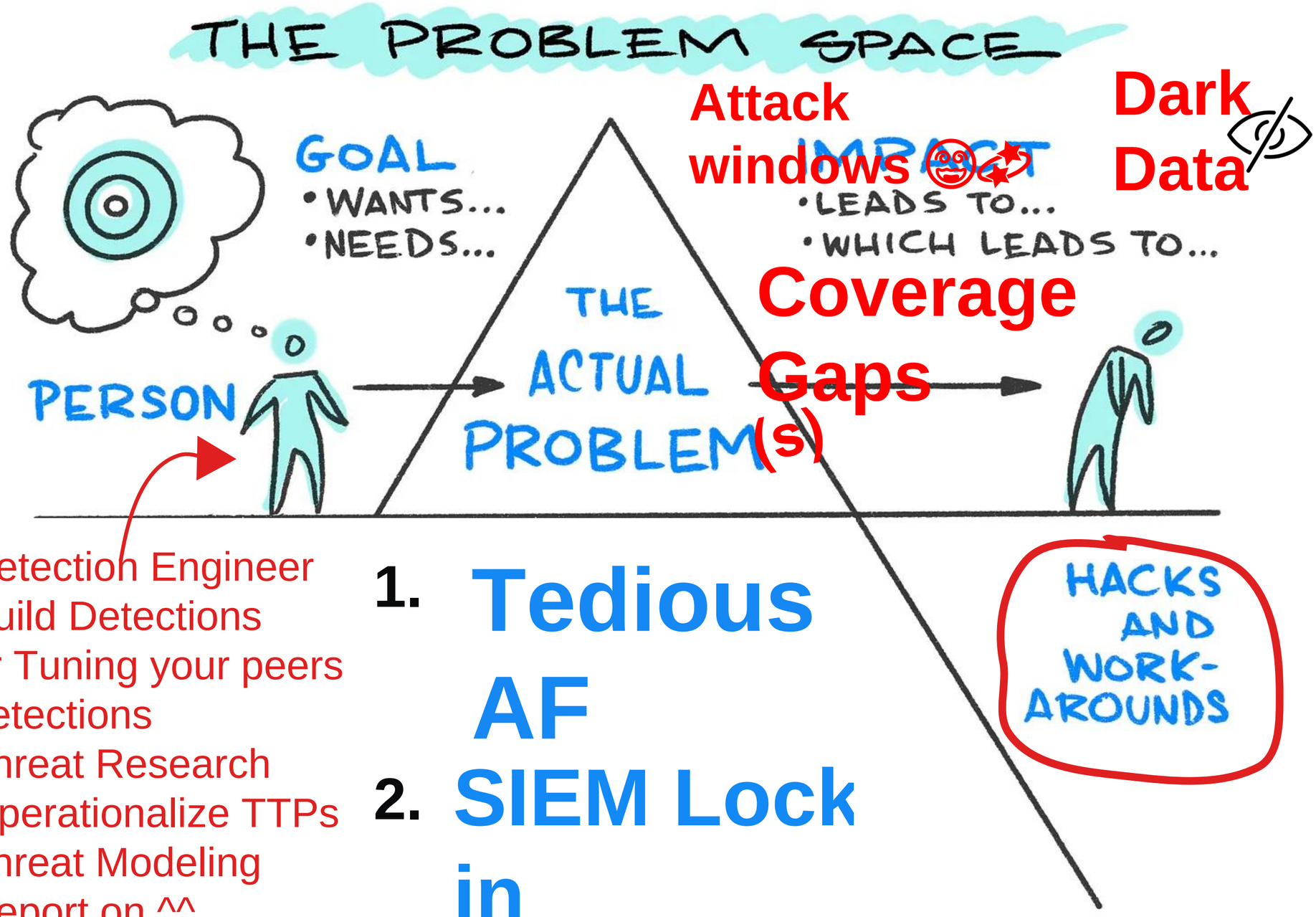
Monolithic Architecture

- Detection Engineering
- Analytics
- Compute
- Storage



Detection Engineer
Build Detections
or Tuning your peers detections
Threat Research
Operationalize TTPs
Threat Modeling
Report on ^^

1. **Tedious AF**
2. **SIEM Lock-in**


THE PROBLEM SPACE
GOAL
• WANTS...
• NEEDS...
PERSON
THE ACTUAL PROBLEM
IMPACT
• LEADS TO...
• WHICH LEADS TO...
HACKS AND WORK-AROUNDS
Attack windows
Dark Data
Coverage Gaps
(s)
Detection Engineer
Build Detections
or Tuning your peers detections
Threat Research
Operationalize TTPs
Threat Modeling
Report on ^^
1. Tedious AF
2. SIEM Lock in

Common Approaches to Deal with Detection Engineering Challenges & SIEM Lock-in

Hire more detection engineers or new point detection tool

Blockers

- Hard to find expertise
- Slow
- Manual
- Creates silos

Optimize the SIEM

Blockers

- Limited improvement
- Also creates silos
- Costly effort required

SOAR playbooks for alert noise

Blockers

- Highly reactive
- Lack MITRE alignment
- Increase in dwell time
- Have to build from scratch

ANVILOGIC™

Advanced Security Operation Centers are able to…

- Quickly scale and adapt to the business and threat landscape
- Leverage the necessary data for threat detection without limitations
- Easily switch tech stacks without disrupting their detection strategy

ANVILOGIC™

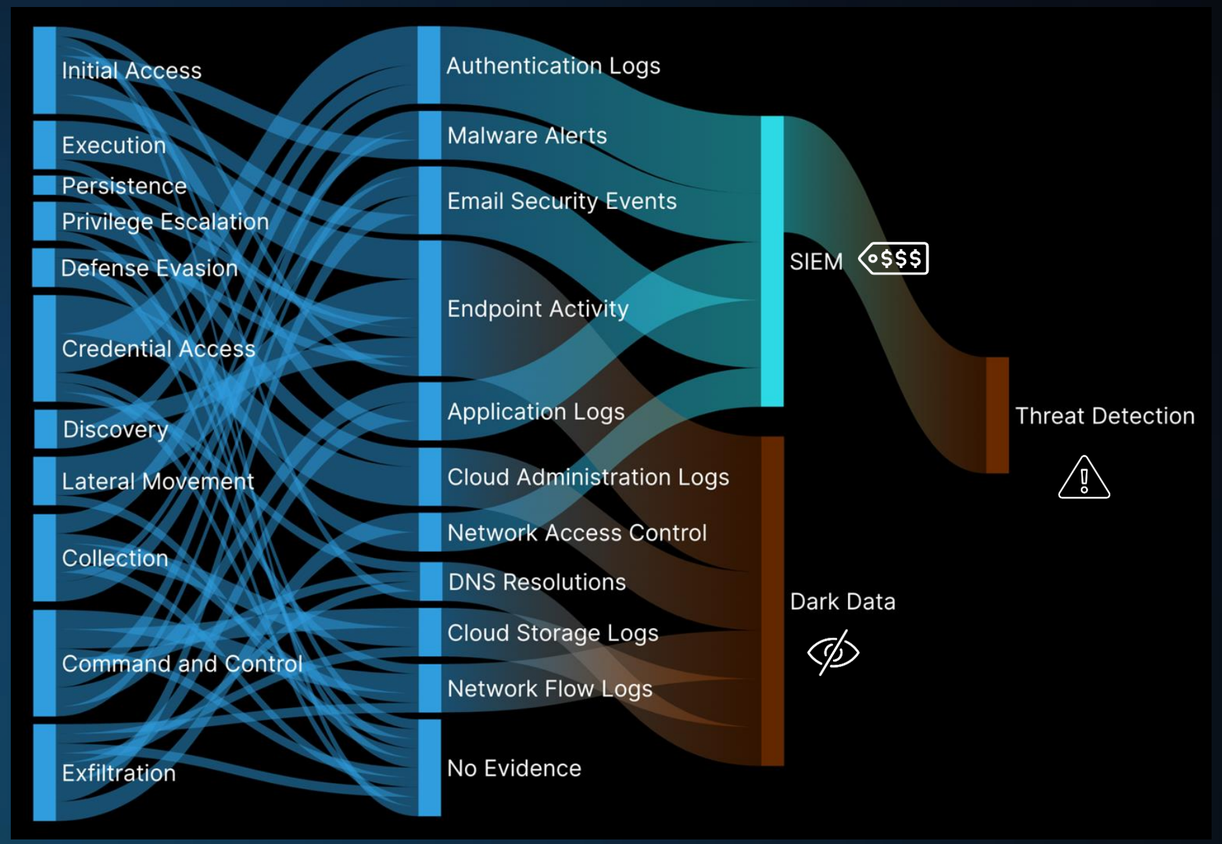
Introducing Anvilogic

The Industry's First & Only
Multi-SIEM Detection Platform

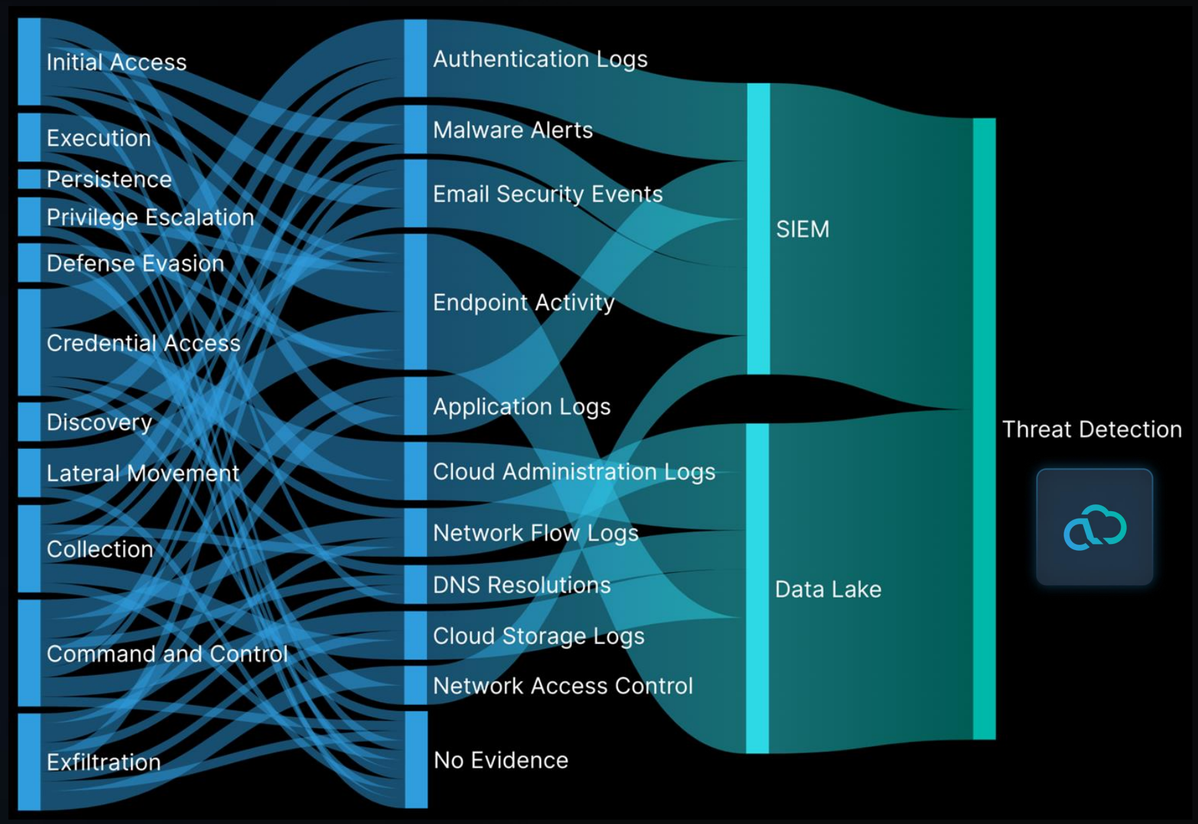
ANVILOGIC™

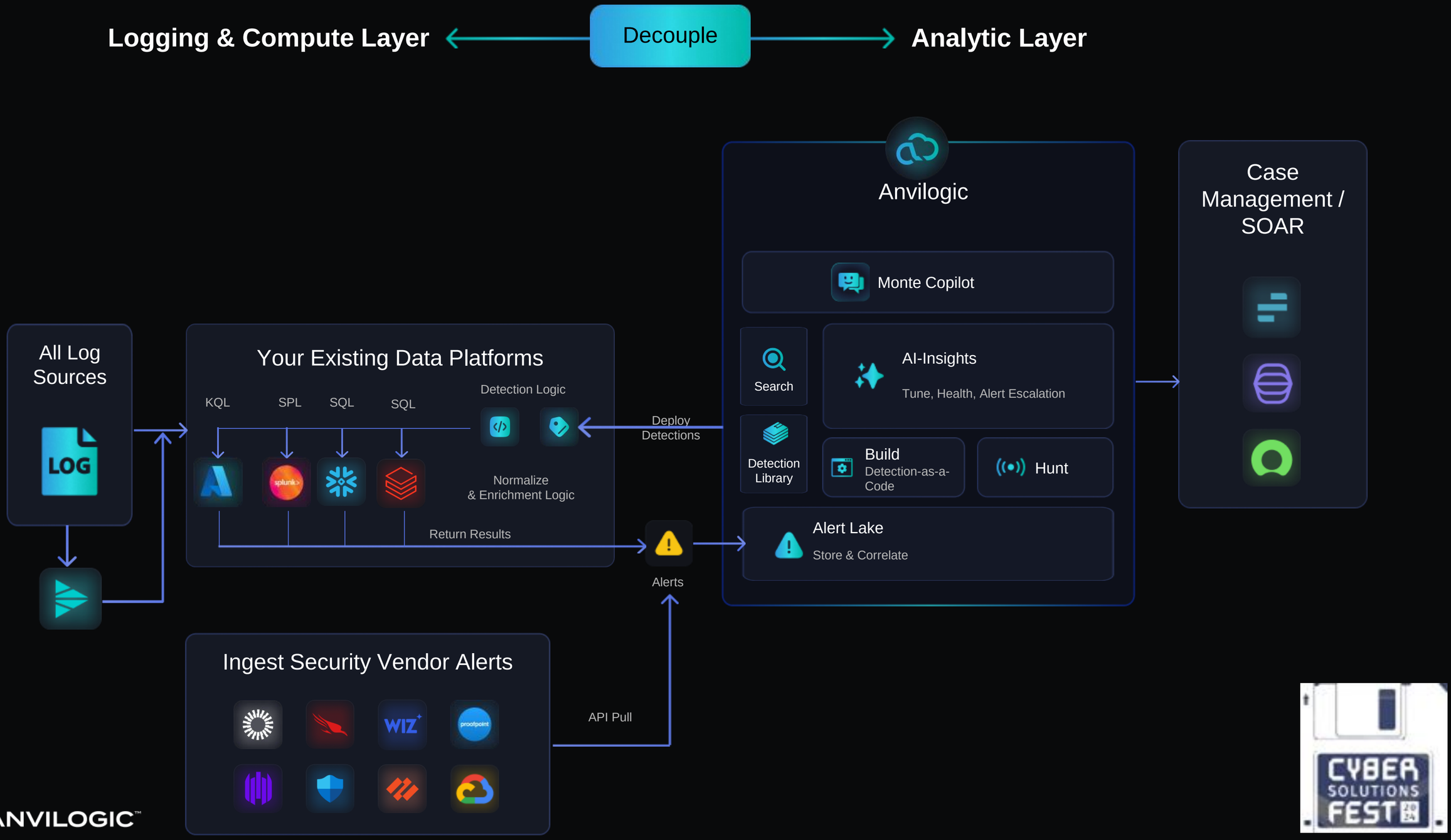
Use Your *Dark Data* For High Fidelity Threat Detection

Monolithic SIEM



Multi-SIEM Detection Platform




Logging & Compute Layer
Decouple
Analytic Layer
All Log Sources
LOG
Your Existing Data Platforms
KQL
SPL
SQL
SQL
Detection Logic
Normalize
& Enrichment Logic
Return Results
Deploy
Detections
Alerts
Anvilogic
Monte Copilot
Search
AI-Insights
Tune, Health, Alert Escalation
Detection
Library
Build
Detection-as-a-
Code
Hunt
Alert Lake
Store & Correlate
Case
Management /
SOAR
Ingest Security Vendor Alerts
API Pull
ANVILOGIC™
CYBER
SOLUTIONS
FEST

ANVILOGIC™

Demo Track

Follow Along with Me

1. Use Case: Detection Creation
    a. Explore our Threat Detection Library
    b. MITRE Coverage Map
    c. AI Recommendations based on data feeds available
2. Use Case: Detection Lifecycle Management
    a. Detection-as-Code
    b. Version Management
    c. Tuning Recommendations
3. Use Case: Measure your Detection Engineering Progress
    a. Continuous MITRE ATT&CK technique coverage scoring
4. Monte Copilot GenAI/LLM SecOps Assistance

Join hundreds of detection engineers and security leaders in the inaugural **2025 Detection Engineering Survey,** conducted in partnership with SANS.

Your valuable insights will uncover the challenges, skill sets, salaries and innovative ideas shaping our field.

Take the **12 minute** survey now.

Take the Survey