# EMPIRICAL

## Empirical Security builds precision AI tuned to your cybersecurity environment

01

### EPSS Model

Empirical builds and maintains the world's only public machine learning model in cybersecurity, EPSS, which is used by over 120 vendors today.

02

### Global Models

Global models combine real-time exploitation telemetry with EPSS predictions to accurately depict exploitation.

03

### Local Models

Local models are trained on your environmental and telemetry data to support your enterprise's decision making.

We're building the world's first local models for cybersecurity, we maintain the world's most advanced global models, and we power existing open-source technology — EPSS.

---

### Enterprises Are Unique. Security Tools Aren't.

Every organization runs its own stack, faces different threats, and operates under different constraints. Yet most security products treat them the same—shipping generic rules and risk scores that ignore local context.

### AI Needs to Be Local, Not Just Large

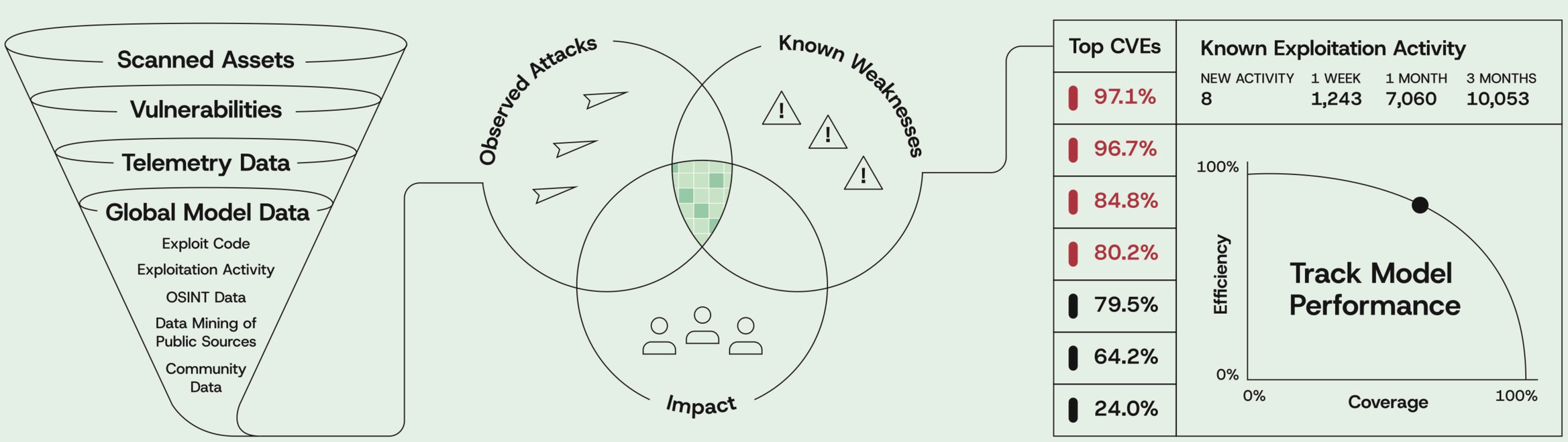
Modern AI enables us to model security posture, asset value, and attacker behavior with real precision—but only if we adapt to the enterprise's actual environment. Local models let us reflect your infrastructure, your priorities, and your risk—not someone else's.

### Static Logic Can't Keep Up

Traditional security tools rely on static playbooks and CVSS scores, producing the same alerts everywhere. That's why teams drown in backlogs while attackers move faster. Local, adaptive models cut through the noise and surface what really matters—for your environment.

## Local Models — How It Works

1. Input your Data
2. Model Runs in Any Cloud
3. API Outputs Real-Time Prioritization



# EMPIRICAL

## Compare Model Features

| ALL MODELS | ALL MODELS | ALL MODELS | ALL MODELS |
|---|---|---|---|
| ☑ EPSS ☑ GLOBAL ☑ LOCAL | ☑ EPSS ☑ GLOBAL ☑ LOCAL | ☑ EPSS ☑ GLOBAL ☑ LOCAL | ☑ EPSS ☑ GLOBAL ☑ LOCAL |
| Predictive Vulnerability Scoring | Hourly Score Updates and Enterprise Support | Legacy Model Support (EPSS v3, v4) | UI and API for Data Discovery & Model Performance |
| **GLOBAL + LOCAL MODELS** | **GLOBAL + LOCAL MODELS** | **GLOBAL + LOCAL MODELS** | **GLOBAL + LOCAL MODELS** |
| ☐ EPSS ☑ GLOBAL ☑ LOCAL | ☐ EPSS ☑ GLOBAL ☑ LOCAL | ☐ EPSS ☑ GLOBAL ☑ LOCAL | ☐ EPSS ☑ GLOBAL ☑ LOCAL |
| Data on over 16,000 exploited in the wild CVEs | Near-Real Time Exploitation Telemetry & Model | ML model for discovering new exploit code on GitHub | All Underlying data contributing to the model exposed |
| **LOCAL MODELS** | **LOCAL MODELS** | **LOCAL MODELS** | **LOCAL MODELS** |
| ☐ EPSS ☐ GLOBAL ☑ LOCAL | ☐ EPSS ☐ GLOBAL ☑ LOCAL | ☐ EPSS ☐ GLOBAL ☑ LOCAL | ☐ EPSS ☐ GLOBAL ☑ LOCAL |
| Custom Vulnerability Model based on your attack telemetry, asset data, vuln data, & threat intelligence | Model Performance Measured against your attack telemetry | Forward Deployed Data Science Team | Only you will have access to your model |

## We bring measurable impact

Past solutions can't prioritize, assess, and handle effective inference at scale.
With Empirical, our models provide understanding and superior prioritization.

**6x**

More efficient than CVSS (comparison vs. EPSS, our free model, at 87% coverage)

**12.4x**

A 1249.04% increase in total exploited CVEs as of January 9th, 2025 compared to CISA Known Exploited Vulnerabilities (KEV)

**23x**

4925 newly exploited CVEs in the last 12 months, compared to 204 in CISA KEV