EMPIRICAL

Empirical Security builds precision AI tuned to your cybersecurity environment

Vault Data Collection

For model development at Empirical Security, several types of data can provide valuable insights and improve the accuracy of both local and global models.

Vulnerability Data

Information about known vulnerabilities (CVEs), exploitability metrics, patching history, and real-world observations of how vulnerabilities are being targeted.
Qualys, Rapid7, Tenable, CrowdStrike Falcon Spotlight, SentinelOne VMS, more

Configuration Data

System and application settings, security controls, misconfigurations, and deviations from best practices that could introduce risk.
AWS Security Hub, MS Defender for Cloud, Wiz Cloud, Lacework, AWS

Endpoint and Host Data

Process execution logs, file system changes, privilege escalation attempts, and endpoint detections that provide context on system behavior.
SentinelOne, Crowdstrike, MS Defender for Endpoint

Threat Intelligence Feeds

Indicators of compromise (IOCs), malware signatures, attacker TTPs (Tactics, Techniques, and Procedures), and threat actor activity.
Recorded Future, Mandiant, FS-ISAC

Exploit and Attack Data

Real-world attack telemetry, pen test results, and honeypot data that provide insight into emerging threats and exploitation methods.
Wiz Cloud, Lacework, MS Defender, Upwind

Incident Response & SOC Data

Historical security incidents, analyst annotations, and remediation timelines that can improve predictive capabilities.
SentinelOne, CrowdStrike, MS Defender for Cloud & Endpoint, AWS Security Hub

Ticketing and CMDB

Historical ticketing related to remediation and urgency, remediation times, and business processes and criticality related to assets.
Jira, ServiceNow, GitLab Security, GitHub Advanced Security

Application Security / DevSecOps

Data about flaws in code, running applications, and third-party components found in the development lifecycle.
Snyk, Semgrep, GitHub Advanced Security, GitLab Security, Checkmarx, more

Identity and Access Management

Environment settings about user identities, resource management, and user permissions.
Okta, Entra ID, AWS IAM Access Analyzer

Custom Data Sources

We can build custom data integrations to match your security and IT operational workflows.

EMPIRICAL

Compare Model Features

ALL MODELS ☑ EPSS ☑ GLOBAL ☑ LOCAL Predictive Vulnerability Scoring	**ALL MODELS** ☑ EPSS ☑ GLOBAL ☑ LOCAL Hourly Score Updates and Enterprise Support	**ALL MODELS** ☑ EPSS ☑ GLOBAL ☑ LOCAL Legacy Model Support (EPSS v3, v4)	**ALL MODELS** ☑ EPSS ☑ GLOBAL ☑ LOCAL UI and API for Data Discovery & Model Performance
GLOBAL + LOCAL MODELS ☐ EPSS ☑ GLOBAL ☑ LOCAL Data on over 17,000 exploited in the wild CVEs	**GLOBAL + LOCAL MODELS** ☐ EPSS ☑ GLOBAL ☑ LOCAL Near-Real Time Exploitation Telemetry & Model	**GLOBAL + LOCAL MODELS** ☐ EPSS ☑ GLOBAL ☑ LOCAL ML model for discovering new exploit code on GitHub	**GLOBAL + LOCAL MODELS** ☐ EPSS ☑ GLOBAL ☑ LOCAL All Underlying data contributing to the model exposed
LOCAL MODELS ☐ EPSS ☐ GLOBAL ☑ LOCAL Custom Vulnerability Model based on your attack telemetry, asset data, vuln data, & threat intelligence	**LOCAL MODELS** ☐ EPSS ☐ GLOBAL ☑ LOCAL Model Performance Measured against your attack telemetry	**LOCAL MODELS** ☐ EPSS ☐ GLOBAL ☑ LOCAL Forward Deployed Data Science Team	**LOCAL MODELS** ☐ EPSS ☐ GLOBAL ☑ LOCAL 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.

17,000+

Known Exploited Vulns (and hourly telemetry about when exploitation occurred)

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

See how your model would differ — book a walkthrough | empiricalsecurity.com | info@empiricalsecurity.com