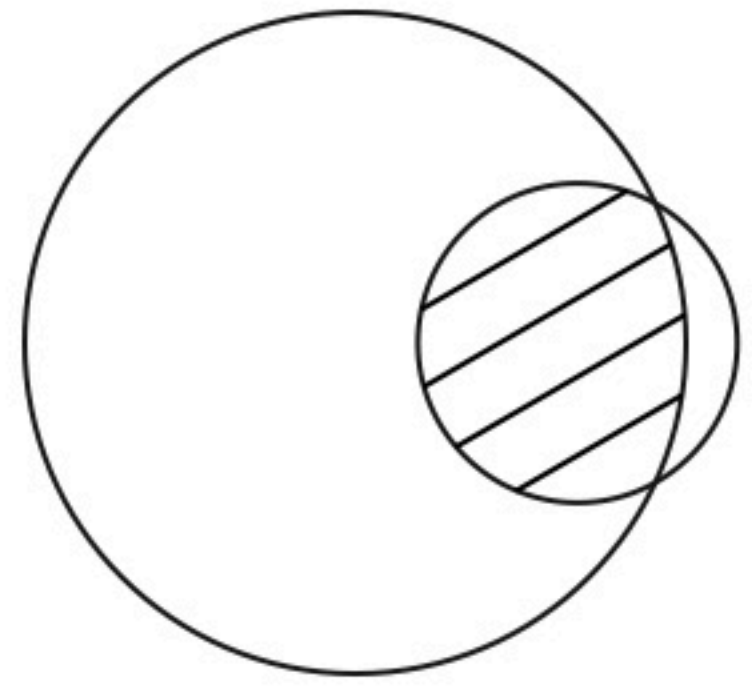




Vault Data Collection

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

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

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

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

Identity and Access Management

Environment settings about user identities, resource management, and user permissions.

Okta, Entra ID, AWS IAM Access Analyzer

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

Threat Intelligence Feeds

Indicators of compromise (IOCs), malware signatures, attacker TTPs (Tactics, Techniques, and Procedures), and threat actor activity.

Recorded Future, Mandiant, FS-ISAC

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

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

Custom Data Sources

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

EMPIRICAL

Foundation Features

The global model

01	02	03	04	05
Predictive scoring based on real exploitation likelihood	380,000+ CVEs covered, 19,000+ confirmed exploited	Near-real-time exploitation telemetry, updated hourly	Backed by a dedicated data science and research team	Full UI and API access

Radiant Features

The local model

Everything in Foundation, plus:	06	07	08
	Custom model trained on your telemetry, assets, configurations, and vuln data	Continuously retrained to reflect changes in your environment	Full data isolation, only you access 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.

19,000+

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

