P3-SEC Cybersecurity Vulnerability Intelligence - Founder Summary

TL;DR

Built a vulnerability prioritization engine combining **NIST NVD + CISA KEV + FIRST EPSS**, analyzing 500 recent CVEs against 1,501 known exploited vulnerabilities.

What This Proves

- **Multi-Source Intelligence** - Integrated 3 federal cybersecurity APIs
- **Risk Prioritization** - Combined CVSS + EPSS + KEV for smart scoring
- **Real-Time Threat Data** - Latest 30 days of published CVEs

Key Metrics

Metric	Value
CVEs Analyzed	500 (last 30 days)
KEV Catalog Size	1,501 known exploited
Critical Severity	5
High Severity	21
Recent KEV Additions	17 (last 30 days)

Top Vulnerability Types (CWE)

CWE	Count	Type

CWE-89	21	SQL Injection
CWE-74	11	Injection
CWE-476	10	NULL Pointer Dereference
CWE-120	8	Buffer Overflow
CWE-434	5	Unrestricted File Upload

Data Attribution

Sources:

- NIST NVD: nvd.nist.gov/developers/vulnerabilities
- CISA KEV: cisa.gov/known-exploited-vulnerabilities-catalog
- FIRST EPSS: api.first.org/epss

DATA DISCLOSURE

> **100% REAL DATA** - All metrics from federal cybersecurity APIs.
> **Important Notes:**
> - 86.6% of CVEs show UNKNOWN severity (awaiting NVD scoring - this is normal for recent CVEs)
> - 0 recent CVEs in KEV (KEV contains confirmed exploited vulns, not new discoveries)
> - EPSS coverage: 14.4% (scores calculated as data becomes available)
> **These limitations reflect real-world vulnerability intelligence timing, not data quality issues.**
