CISCO
SECURE

# Transforming Vulnerability Management

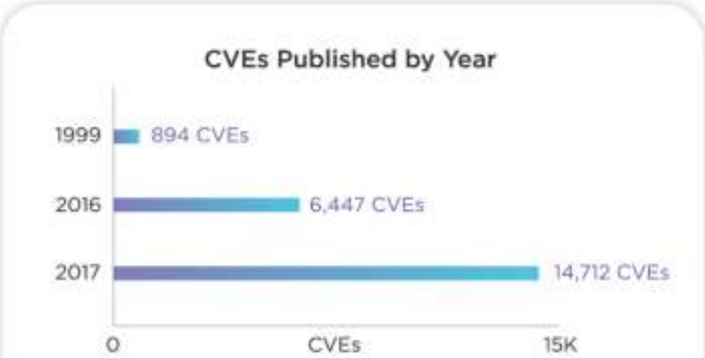
## Benefits of a risk-based Vulnerability Management approach

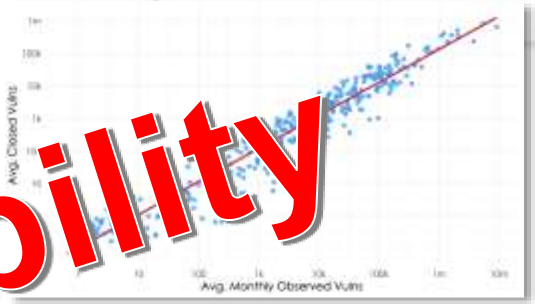
Rene Straube
Technical Solution Architect, Cisco Kenna Security
IT-SA, October 2022

The bridge to possible

# The Vulnerability Problem

- Number of Vulnerabilities increase by 15 to 20% per year
- Organizations are able to fix less than 20% of found Vulnerabilities





Exploitability

- Problem: The number of existing open vulns actually do not change!
  - How can an organization be successful and efficient with VM?
  - What's a helpful measure to prioritize VM efforts?
  - What is a meaningful benchmark for success in VM?

# Why Exploitability of Vulnerabilities is relevant?

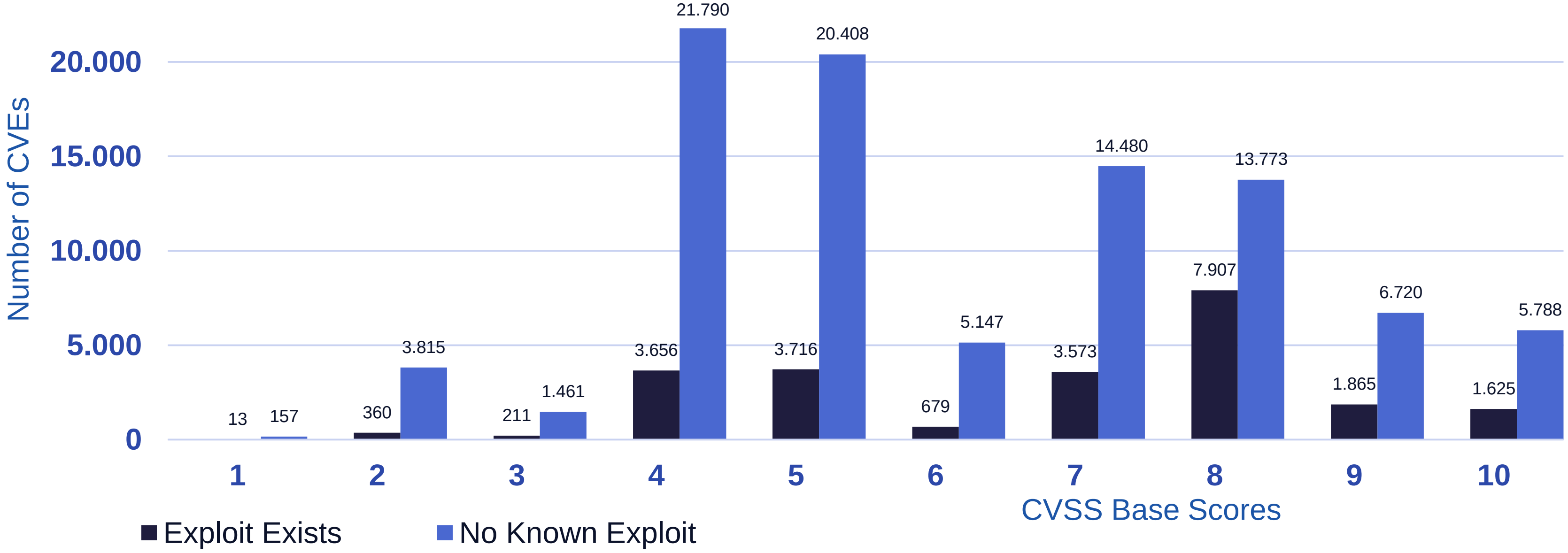
- **Exploitability:**
  What’s the likelihood that a given vulnerability will be exploited within a window of time?
- Kenna Security, the Cyentia Institute, and a few other organizations have been collaborating on this exact thing
  - Exploit Prediction Scoring System (EPSS), maintained by a Special Interest Group at FIRST.org
  - EPSS is an open, data-driven effort for predicting whether and when vulnerabilities will be exploited in the wild https://www.first.org/epss/
- Cyentia also performed a real-world analysis of 3 billion vulnerabilities managed across 500+ organisations and 55 sources of external intelligence
  - This research is also leveraging Kenna’s Vulnerability Intelligence
  - Results: https://www.kennasecurity.com/research/
- Key Findings for Exploitation Relevance
  - The chance of a vulnerability being exploited in the wild is 7X higher when exploit code exists
  - The volume of exploitation detections jumps five-fold upon release of exploit code

**Exploitability**
**= Risk**

# What about CVSS?

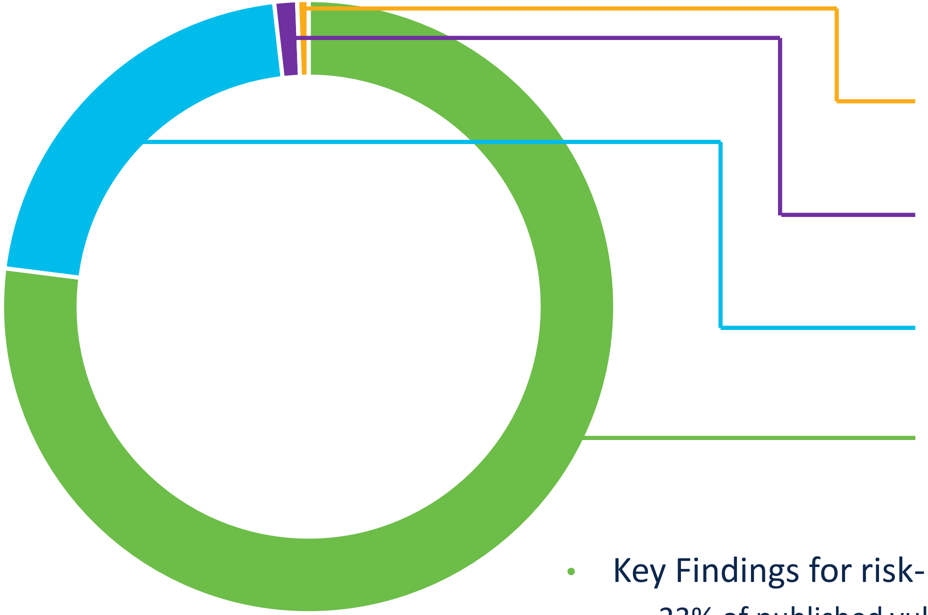
## A Poor Predictor of Exploitability

- CVSS is a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity
- Most reported vulnerabilities are never acted upon by hackers



Source: Kenna / Cyentia

# Most vulns are never exploited



**0.6%** of CVE’s just have executed exploits in the wild

**1.2%** of CVE’s have published and observed exploits

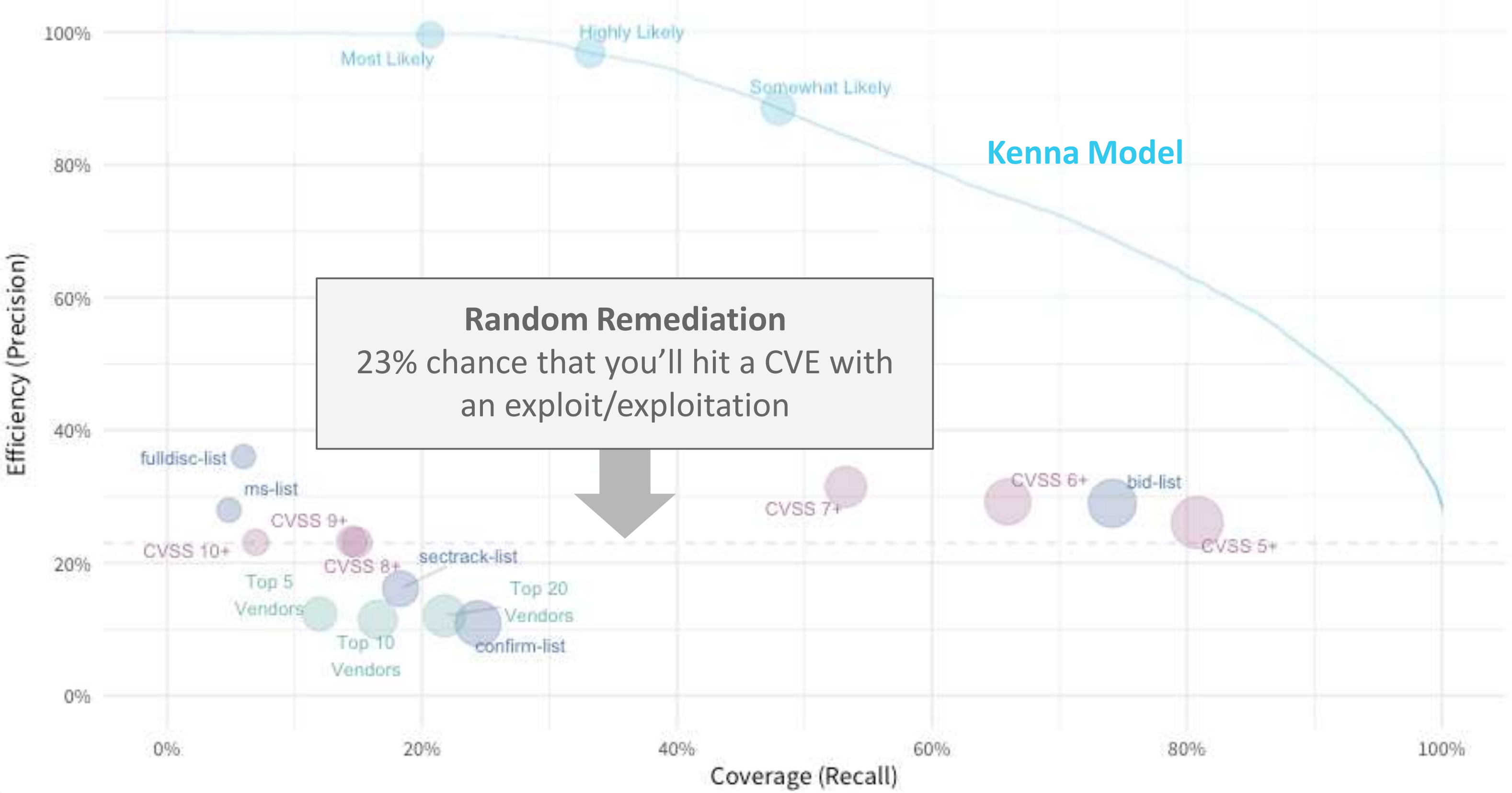
**21.2%** of CVE’s just have an exploit publicly released

**77%** of CVE’s have no published or observed exploit

- Key Findings for risk-based Vulnerability Prioritization
  - 23% of published vulnerabilities have associated exploits or exploit code
  - Less than 2% of published vulnerabilities have observed exploits in the wild

Comparison of CVEs with exploit code and/or observed exploits in the wild relative to all published CVEs
*Source: Kenna / Cyentia*

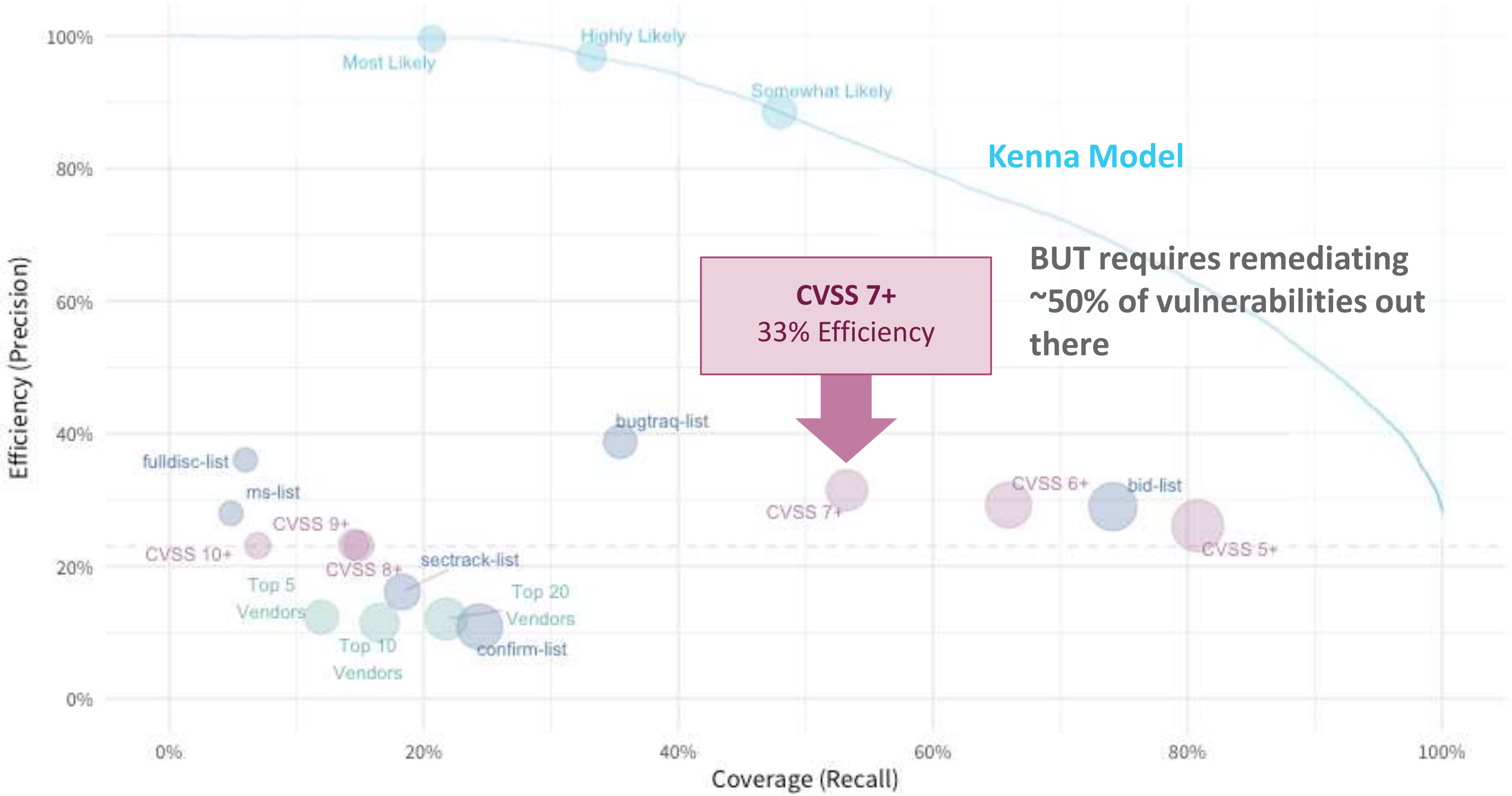
# What is Your Vulnerability Management Strategy?



Kenna Model

**Random Remediation**
23% chance that you'll hit a CVE with an exploit/exploitation

# What is Your Vulnerability Management Strategy?



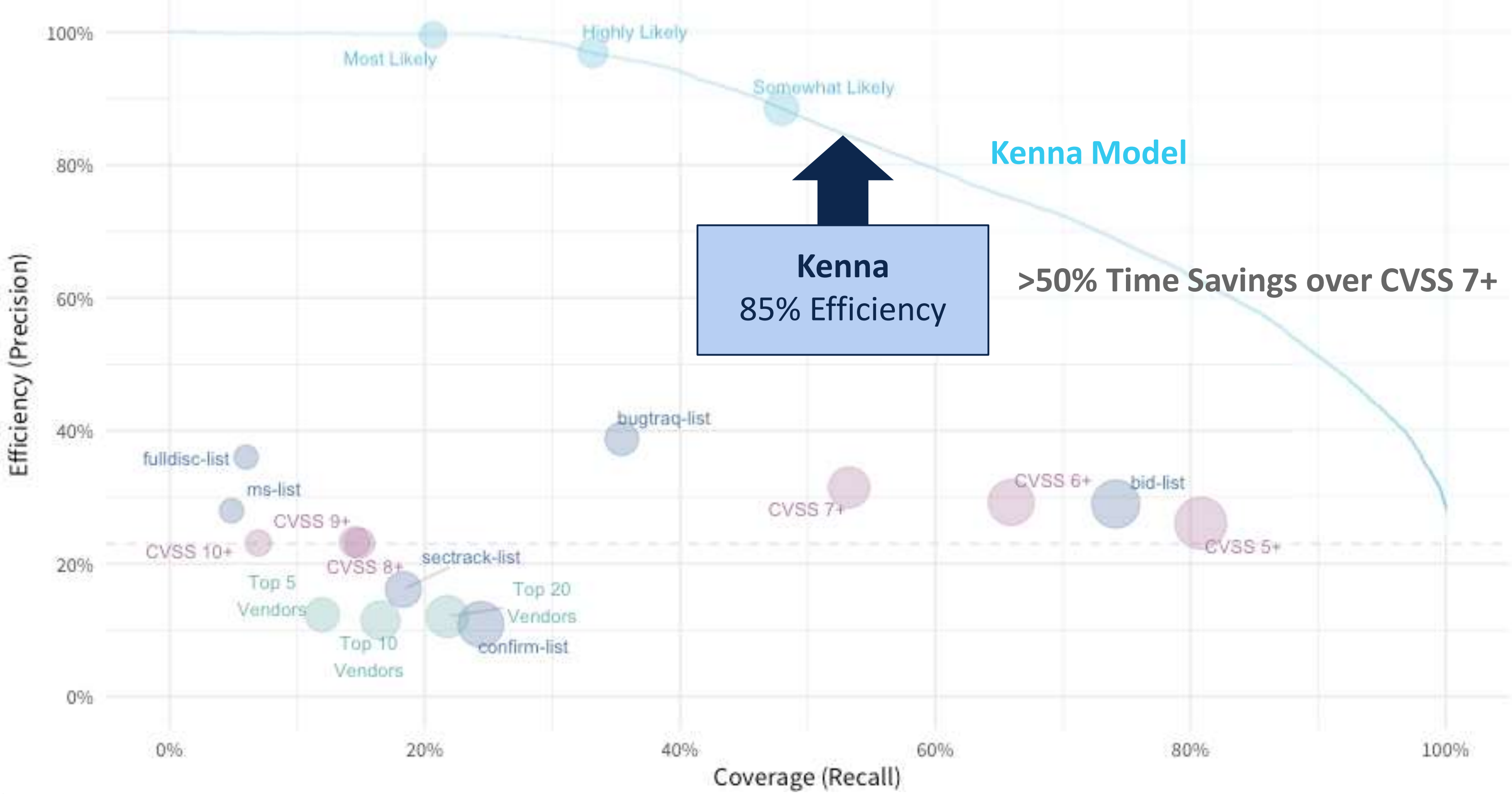
Kenna Model

**CVSS 7+**
33% Efficiency

**BUT requires remediating ~50% of vulnerabilities out there**

CISCO SECURE

# What is Your Vulnerability Management Strategy?



**Kenna Model**

**Kenna**
85% Efficiency

**>50% Time Savings over CVSS 7+**

# Kenna’s Ground Truth Telemetry

## Real-Time Global Exploit Intelligence

### Extensive Threat and Vulnerability Data

- ✓ 18+ threat and exploit intelligence feeds
- ✓ 12.7+ billion managed vulnerabilities
- ✓ 1+ billion security events processed monthly

### Exploit Intelligence

- Canvas Exploitation Framework
- Contagio
- D2 Elliot
- Exploit DB
- Github Exploit Feed: Cyentia Institute
- Metasploit
- ReversingLabs
- Proofpoint
- Secureworks CTU
- Black Hat Kits on rotation

### Threat Intelligence

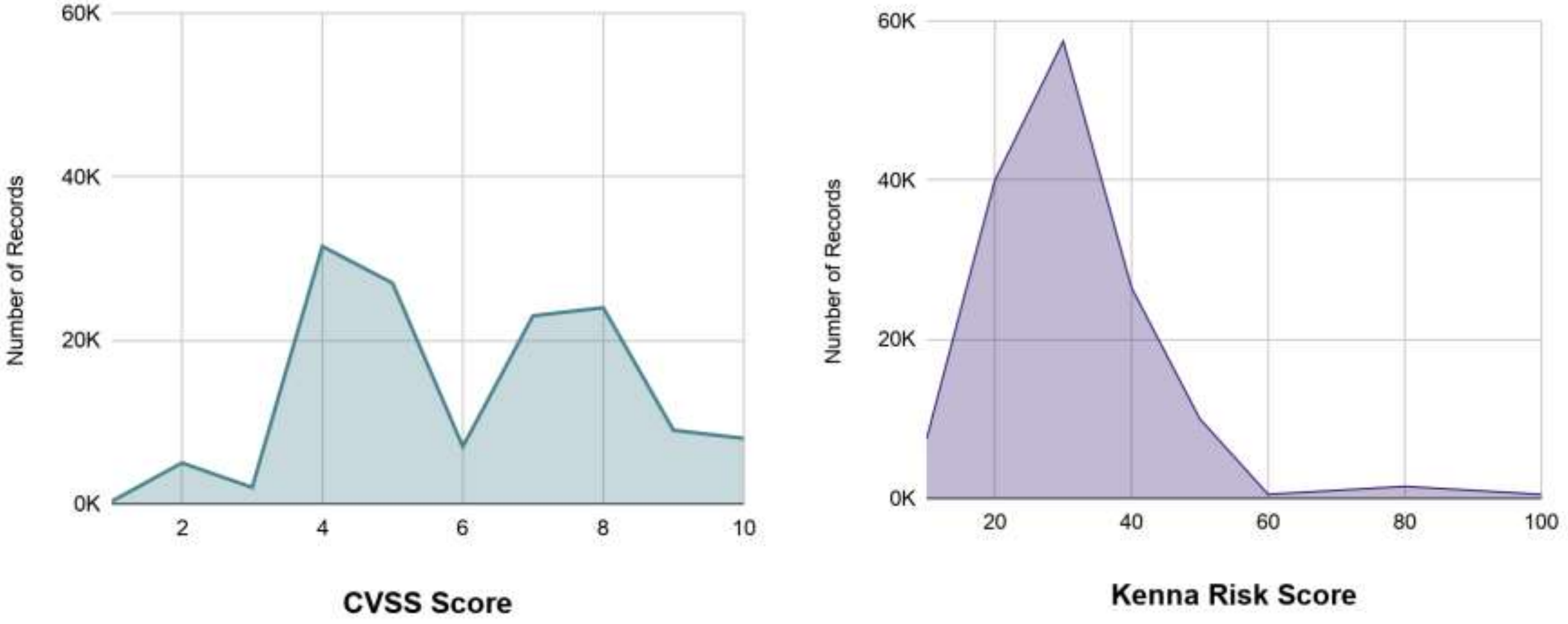
- Alienvault OTX
- Alienvault Reputation
- Emerging Threats
- Exodus Intelligence
- ReversingLabs
- Sans Internet Storm Centre
- Secureworks CTU
- Silobreaker
- X-Force Exchange

**Data Science**

**Machine Learning**

**Predictive Modeling**

# Fewer High-Risk Vulns to Remediate



**Kenna Risk Score vs. CVSS**
(All CVEs, All Time)

# CVSS, Vulnerability Scanner, and Kenna Comparison

## If Everything is a Priority, Nothing is.

| | Total Vulnerabilities: 468,954 | | |
|---|---|---|---|
| | Low | Medium | High |
| CVSS | 1 - 3 | 4 - 6 | 7 - 10 |
| | 32,734 | 180,202 | **256,018** |
| Scanner A | 1 | 2 - 3 | 4 - 5 |
| | 6,753 | 93,139 | **369,062** |
| Kenna | 0 - 33 | 34 - 66 | 67 - 100 |
| | 321,249 | 139,194 | **8,511** |

**Highlights**

**CVSS**
**>50% of all is Prioritized**

**Scanner A**
**>60% of all is Prioritized**

**Cisco Kenna**
High Vulns only **1.8%** of Total

**651** High Vulns found by Kenna that are not considered high by Scanner A

**604** High Vulns found by Kenna that are not considered high by CVSS

# Cisco Kenna - Key Features and Functionality

### Efficient Decisions
Identify the vulnerabilities
that will truly reduce your cyber risk.

### Centralized Management
Pull in data from existing tools, like
scanners, CMDB,
and more.

### IT Self-Service
Enable IT teams to understand
what to remediate, why, and how.

### Metrics-Based Reporting
Deliver clear, effective reports with
quantifiable metrics.

### Peer Benchmarking
Compare your risk posture with that
of your industry peers.

### Risk-Based SLAs
Set intelligent SLAs based on your
risk tolerance.

cisco
SECURE

# Secure your resilience.

cisco The bridge to possible