

CISCO
SECURE



Info Quest
TECHNOLOGIES

CISCO
Partner
Distributor

Kenna:

*How to de-risk your Vulnerabilities and
Save your precious time!*

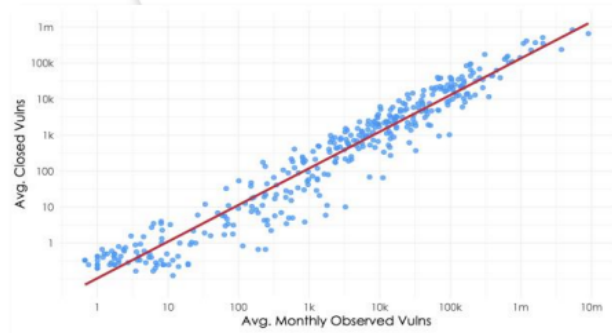
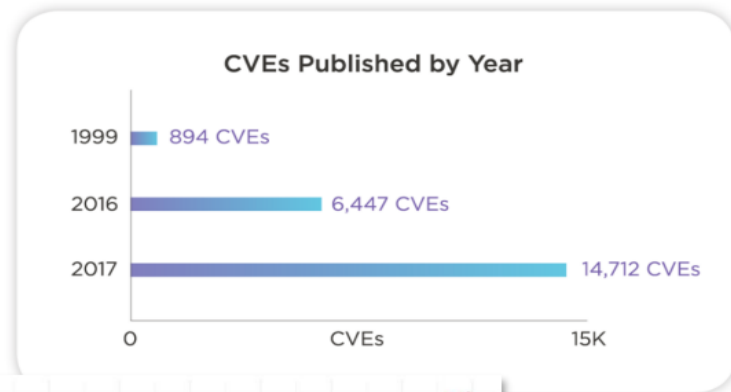
Evi Kastania – Info Quest Technologies Senior Presales Engineer

Konstantina Syntila – Cisco Cyber Security Sales Specialist Leader GR/PT

26th April 2023

The Vulnerability Problem

- Number of Vulnerabilities increase by 15 to 20% per year
- Organizations are able to fix less than 20% of found Vulnerabilities
 - Issue #1: Prioritization is a MUST!
 - Issue #2: Number of Vulns is constant!

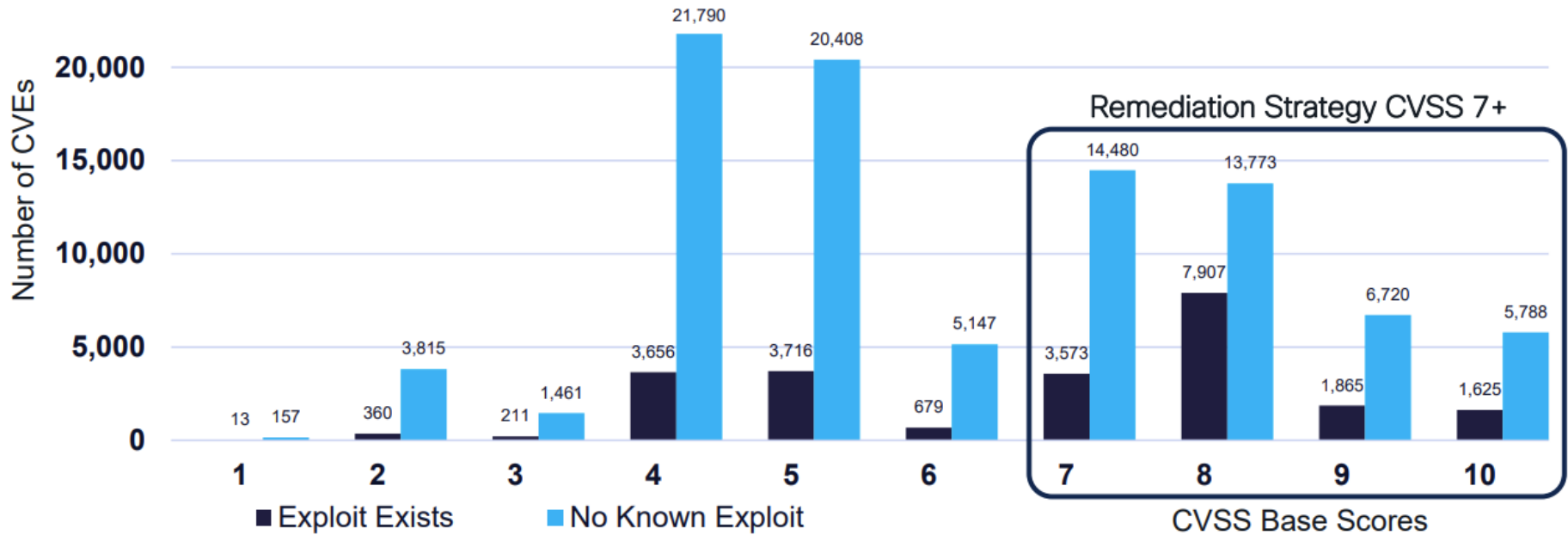


- If the number of existing open vulns actually do not change ...
 - What's a helpful measure to prioritize vulnerability remediation efforts?
 - What is a meaningful benchmark for success in VM?

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
- BUT, most reported vulnerabilities are never acted upon by hackers

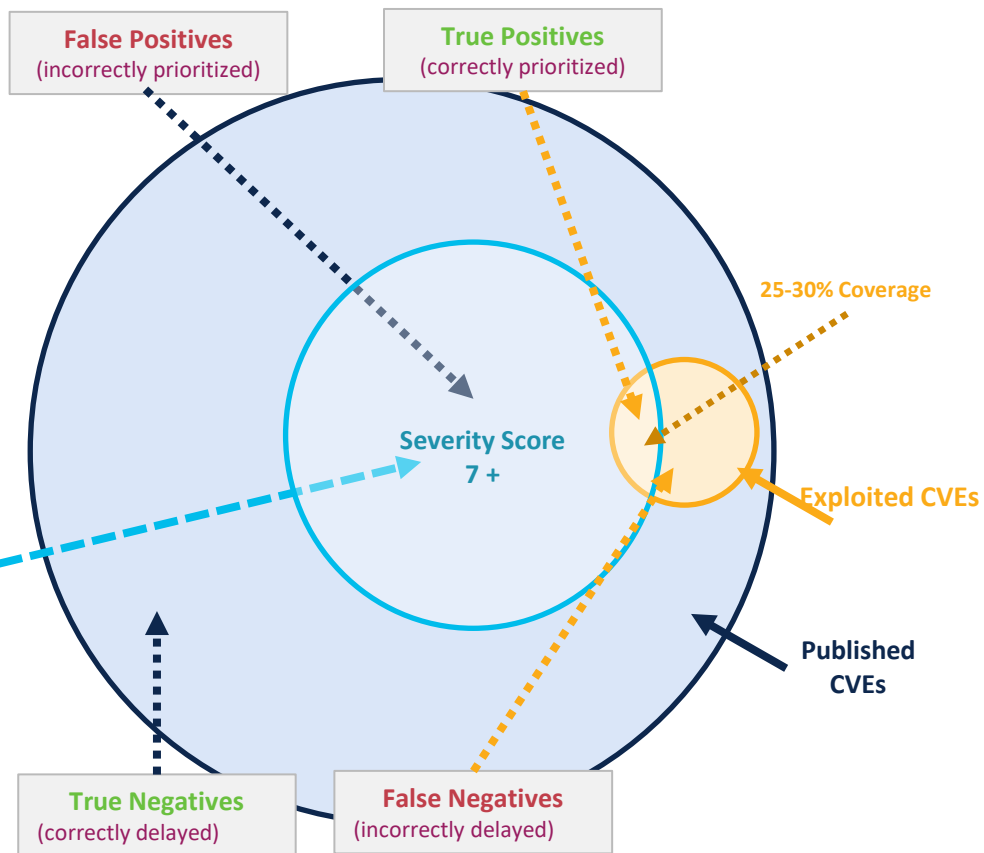


A Wicked Problem

Somewhere between 2-5% of CVEs are (detected as) exploited in the wild.

How do we prioritize these?

How does CVSS help?



Exploitability = Risk

- **Exploitability:** The likelihood that a given vulnerability will be exploited within a window of time
- **Exploit Prediction Scoring System (EPSS)** is an open, data-driven effort for predicting whether and when vulnerabilities will be exploited in the wild
<https://www.first.org/epss/>
- **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

Based on real-world analysis of 3 billion vulnerabilities managed across 500+ organisations and 55 sources of external intelligence

source: <https://www.kennasecurity.com/research/>



Risk Based Vulnerability Management

To efficiently reduce cybersecurity risk using the transformative power of data science.

A Model for Predicting Exploitation

“A prediction model is inherently forward-looking.


In other words, we must be able to identify CVEs as likely candidates for exploitation even though they have not yet been targeted by attacks or developed into exploit code.”

KENNA
Security

119
Cyentia
INSTITUTE

Cloudy with a Chance of Exploits

VulnTV Weather Forecast



On Wednesday, there's a 90% chance of rain.




“Wednesday”



Cloudy with a Chance of Exploits

A Predictive Model



There's a 90% chance of XYZ vulnerability becoming weaponized.



Weaponization Occurs

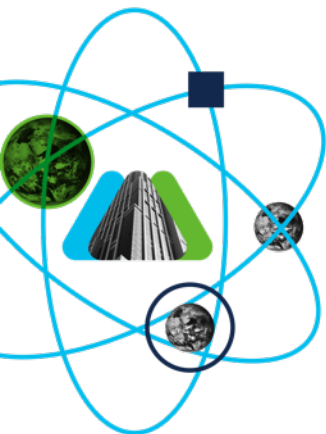


Fun Fact: Kenna can predict the weaponization of a vulnerability with 94% accuracy.

What is behind KENNA prediction model?

Kenna looks at various categories of vulnerability data to understand what happens to a CVE during all stages of its life, from the assignment of a CVE to the unlikely event of an exploitation in the wild.

Volume & velocity data is different than a “Yes/No” data point. It tells you: *In the past 24 hours, 7240 machines have been exploited using a CVE.*



Data Categories

MITRE & NVD
Vulnerability Scoring
Early Warning Chatter

Exploit Databases
Malware Analysis

Threat Actors
Malware Families

Volume & Velocity of
Exploitation in the Wild

Machine Learning Model-Based Risk Scoring

This incorporates the **prediction** of exploitation publication and exploitation event (94% accuracy)



Telemetry behind the scenes?

+18 threat and exploit intel feeds

+12.7B managed vulnerabilities

+1B security events processed monthly



Exploit Intel

Canvas Exploitation Framework

CISA Known Exploited Vulnerabilities

Contagio

D2 Elliot

Exploit DB

Github Exploit Feed: Cyentia Institute

Metasploit

ReversingLabs

Secureworks CTU

Black Hat Kits on rotation

Threat Intel

Alienvault OTX

Alienvault Reputation

Cisco Talos

Emerging Threats

ReversingLabs

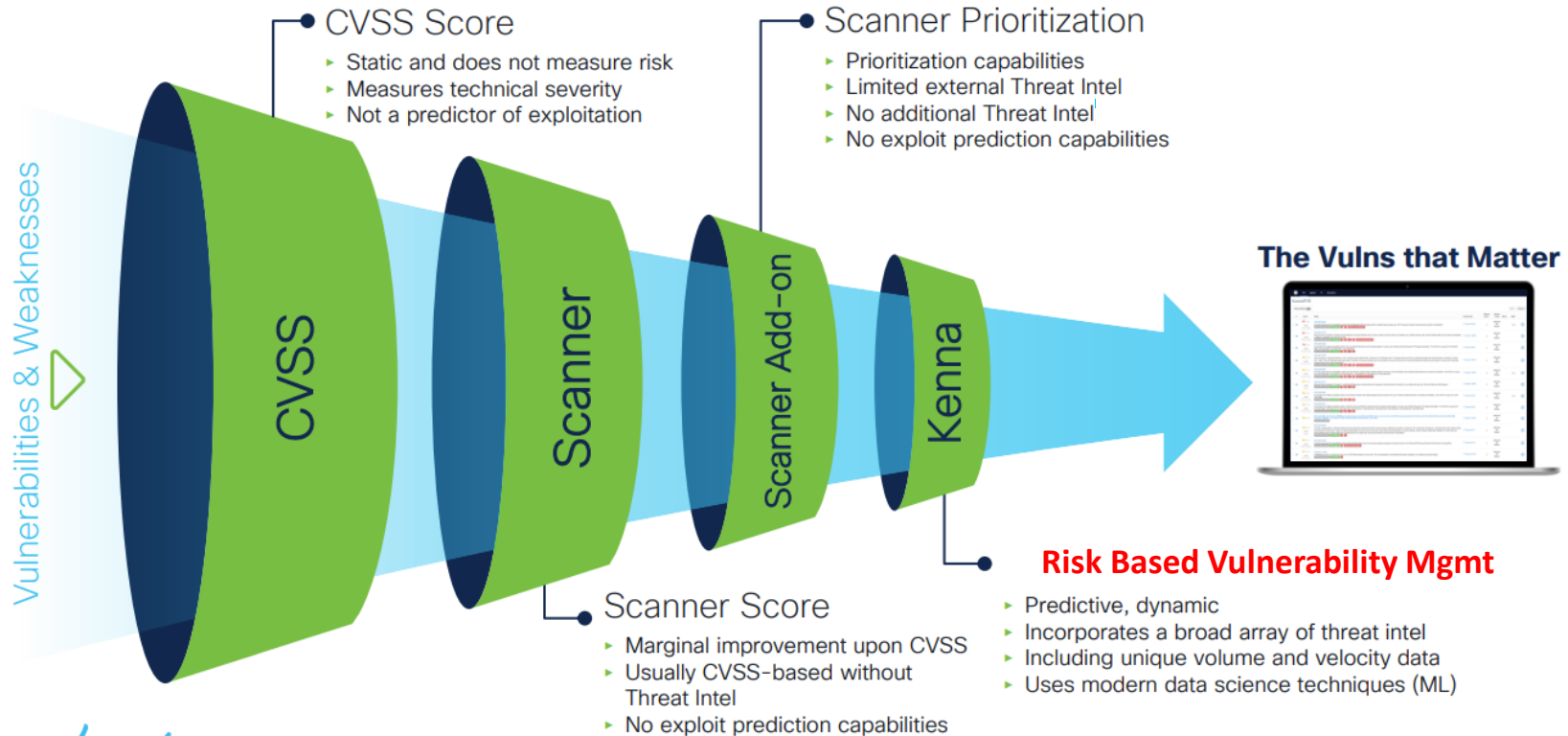
Sans Internet Storm Centre

Secureworks CTU

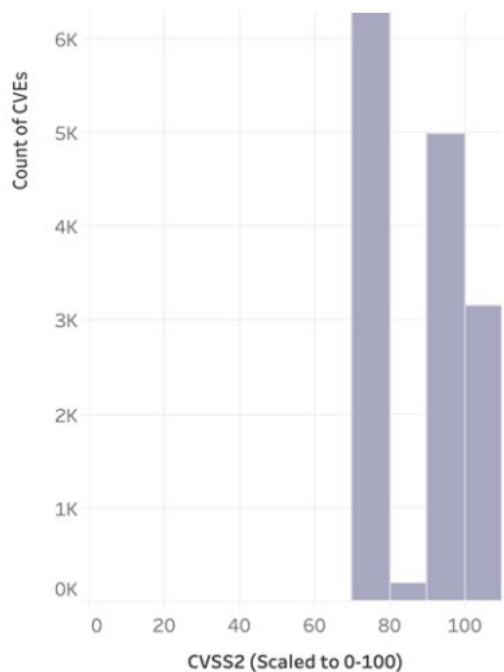
Silobreaker

X-Force Exchange

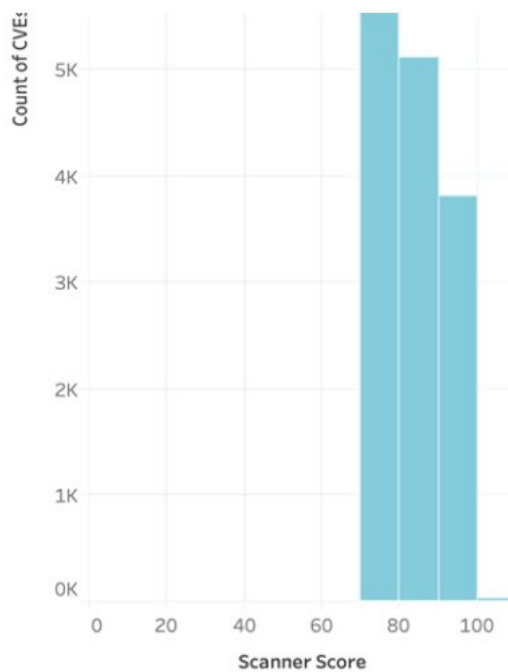
Risk Based prioritization: Highlighting the real risk



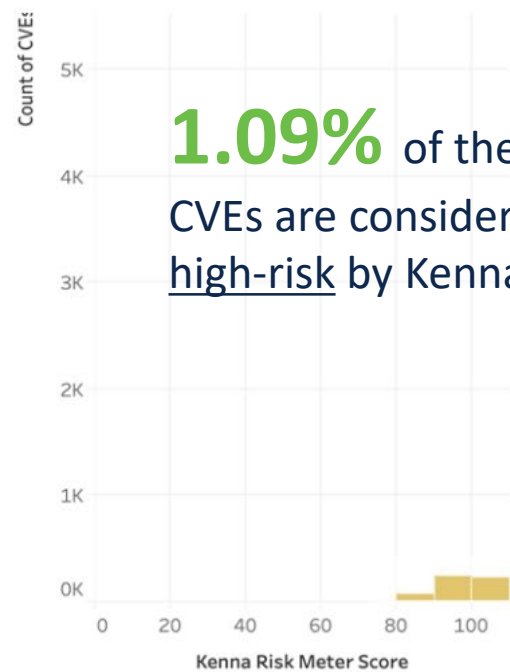
RBVM risk score vs. other strategies



17,279 CVEs to remediate



15,215 CVEs to remediate



1.09% of these
CVEs are considered
high-risk by Kenna

627 CVEs to remediate

Integrate with your existing security tools

Technology integrations with 50+ vendors





**After working with the world's
most demanding businesses
over the past 10 years**



Cisco Principles for Responsible AI

Transparency

Fairness

Accountability

Privacy

Security

Reliability

Responsible AI at trust.cisco.com.

Info Quest
TECHNOLOGIES


cisco
Partner
Distributor


cisco **SECURE**

THANK YOU!