VULNERA
February 28, 2024

Navigating the Maze

Making Sense of Vulnerability Risk Indicators

Raffi Erganian, Cofounder – VULNERA

Who We Are

Raffi Erganian

VULNERA

OPTIV

ACCUVANT

BOEING

Joe Luna

VULNERA

EarthLink

UNITED ONLINE

FedEx Kinko's

Who We've Helped

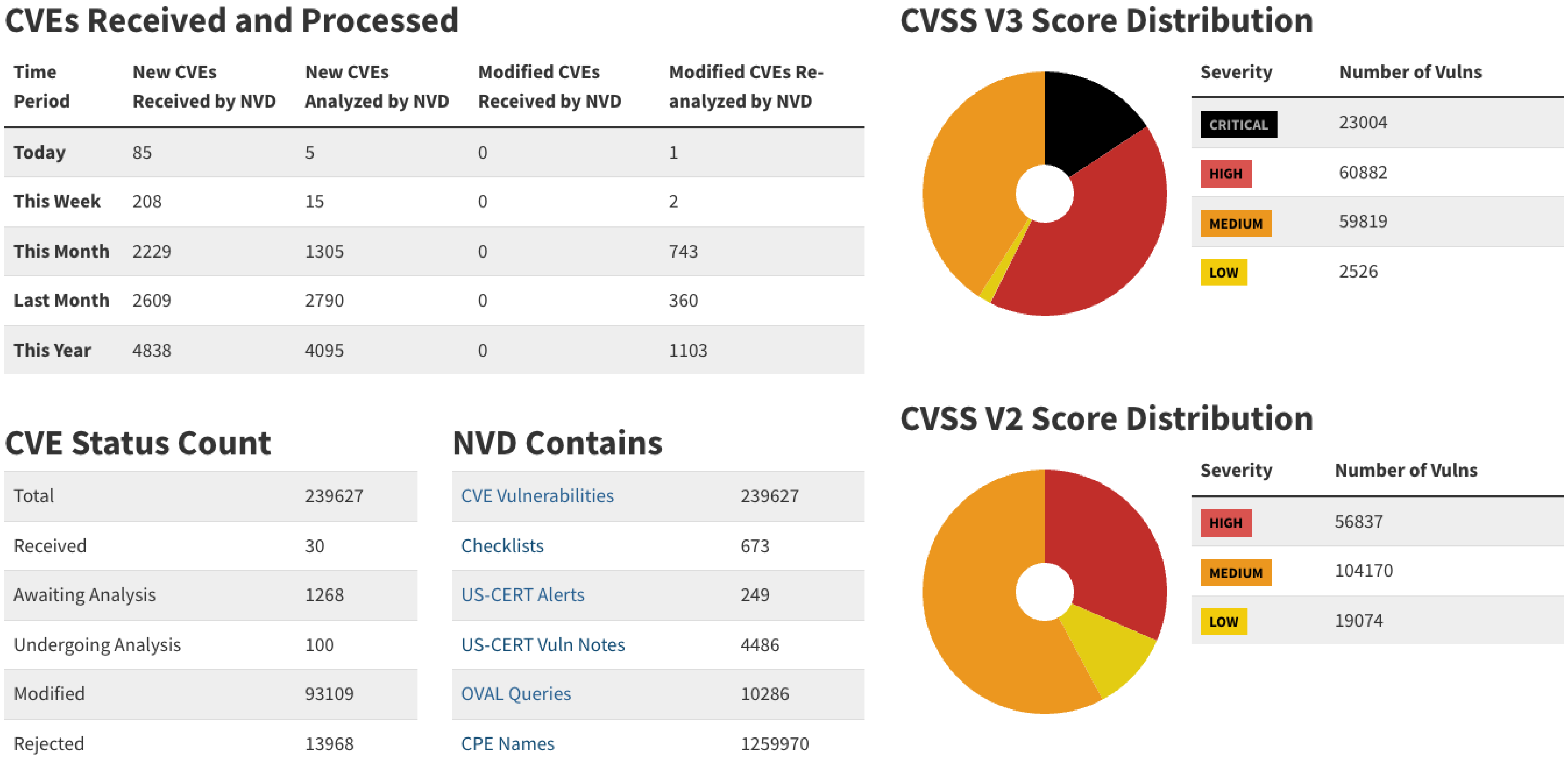
United States Federal Reserve System
amazon
CBRE
VISA
APRIA
Reverb
THE MLS.com
County of Los Angeles California
CVS
eharmony
TASTEMADE
CIT
GYMBOREE
KORN FERRY
OLYMPUS
RUGER
Sterno
BLACK+DECKER
HONDA
open bank
SEPTA
Viasat
houzz
HCVT
HOLTHOUSE | CARLIN | VAN TRIGT LLP
tyco
SDSC
SAN DIEGO SUPERCOMPUTER CENTER
DFW
LENNAR
Baxter

What we’ll cover

- Vulnerability Context
- NVD Challenges
- The Tools
- Lagging Indicators
- Prioritization
- Easy Wins

Vulnerability Context

NVD Dashboard



CVEs Received and Processed

Time Period	New CVEs Received by NVD	New CVEs Analyzed by NVD	Modified CVEs Received by NVD	Modified CVEs Re-analyzed by NVD
Today	85	5	0	1
This Week	208	15	0	2
This Month	2229	1305	0	743
Last Month	2609	2790	0	360
This Year	4838	4095	0	1103

CVE Status Count

Total	239627
Received	30
Awaiting Analysis	1268
Undergoing Analysis	100
Modified	93109
Rejected	13968

NVD Contains

CVE Vulnerabilities	239627
Checklists	673
US-CERT Alerts	249
US-CERT Vuln Notes	4486
OVAL Queries	10286
CPE Names	1259970

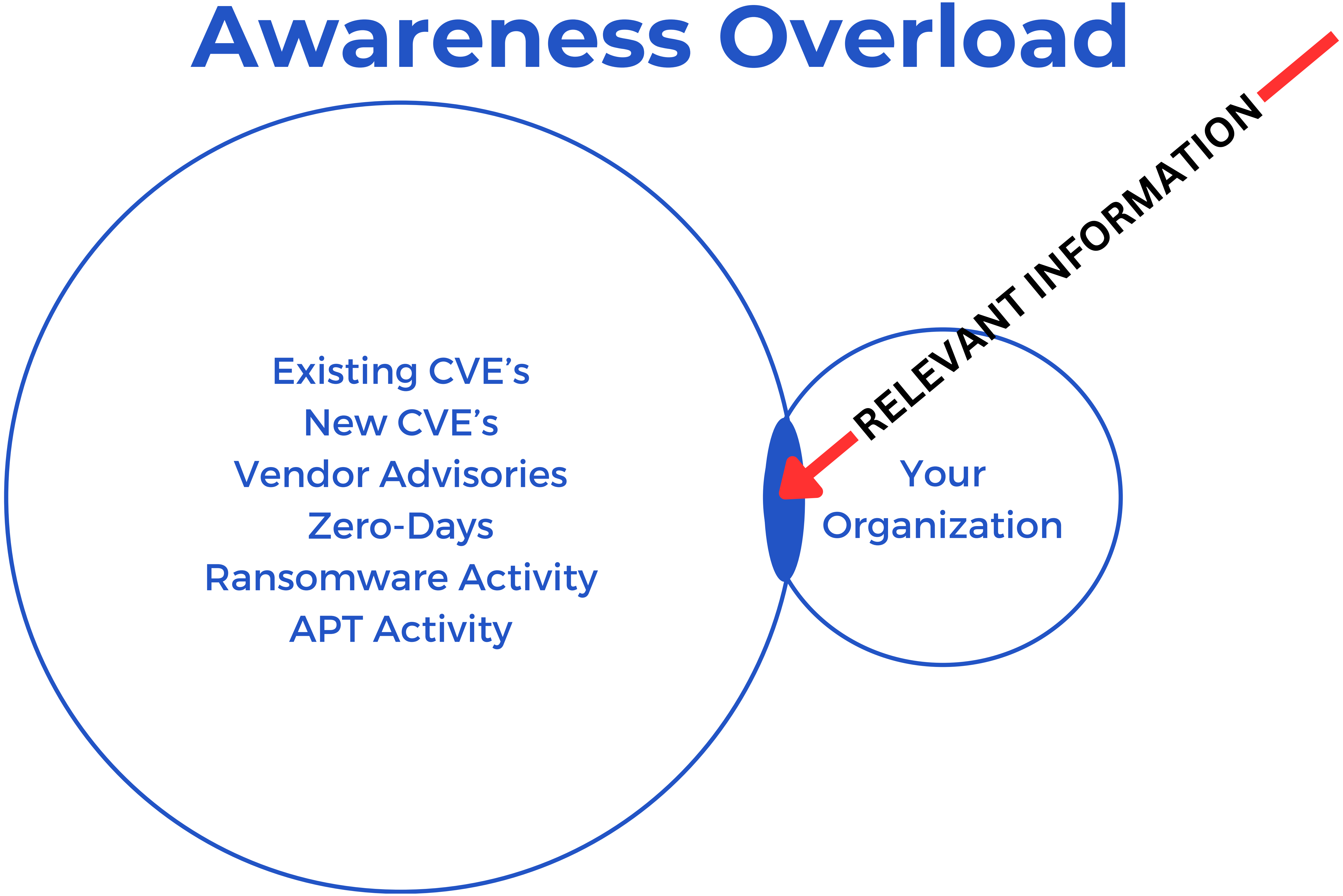
CVSS V3 Score Distribution

Severity	Number of Vulns
CRITICAL	23004
HIGH	60882
MEDIUM	59819
LOW	2526

CVSS V2 Score Distribution

Severity	Number of Vulns
HIGH	56837
MEDIUM	104170
LOW	19074

Awareness Overload



Existing CVE’s
New CVE’s
Vendor Advisories
Zero-Days
Ransomware Activity
APT Activity

Your Organization

RELEVANT INFORMATION

Tools at our disposal

Industry, community, and vendor risk ratings/metrics

NVD, CVE, CVSS, CWE

CISA KEV, EPSS

Vendor Ratings

NIST & The NVD

The industry standard repository for vulnerabilities

CVSS

CWE

Delay

Accuracy

LAGGING INDICATORS

Exposure Window and Risk Tolerance

- Delayed Response
- Missed Opportunities for Mitigation
- False Sense of Security
- Compliance Risks

19 days

CISA KEV

44 days

EPSS

23 days

Scanners

Live Demo

Stop reducing vulnerability risk to a single score.

Prioritizing

Reducing the noise

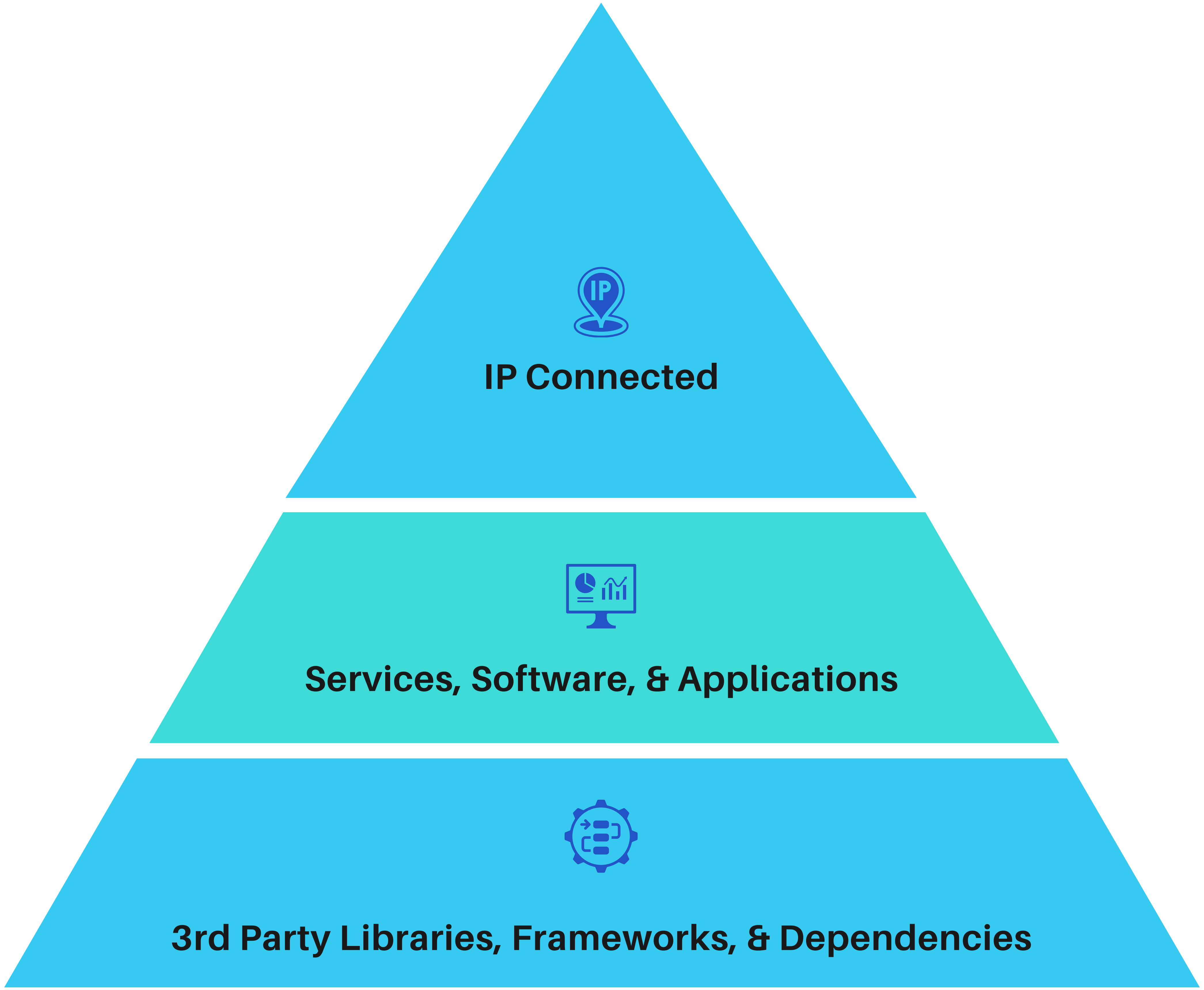
Know Your Assets

NVD, CVSS, & CWE

CISA KEV / News / VIP-TIP

EPSS?

Know Your Assets



IP Connected

Services, Software, & Applications

3rd Party Libraries, Frameworks, & Dependencies

Vulnerability Prioritization

Awareness with Insight drives Action

Awareness

News, Peers, Advisories, NVD, CISA KEV, etc

Insight

Deployed solutions & technologies

Action

Policies, Procedures & Playbooks

Catalyst

Awareness vs Technology Based Signals

Awareness

Awareness requires legwork.

You need to keep a pulse on what's happening.

NVD
Advisories
CISA

News

TIP/VIP

Peers & Social Media

Insight

What tools can you rely on for insight?

Asset Inventory

Software Inventory

Vulnerability Scanners

SBOM

Challenges

Insight is useless without **Awareness**

Awareness inactionable without **Insight**

No action without **Insight + Awareness**

Insight Pitfalls

Schedule

Would you run AV once a week?

Agents

False negatives, unsupported assets

Port Coverage

False negatives, skipping ports

Excluded Checks

Missing valuable insight

Easy Wins

CNAs & Vendor Advisories

CVSS & CWE

Leverage TIP/VIP

Easy Wins

Asset & Software Inventory

Edge Device/App List

Vulnerability Scanning

SBOM

Easy Wins

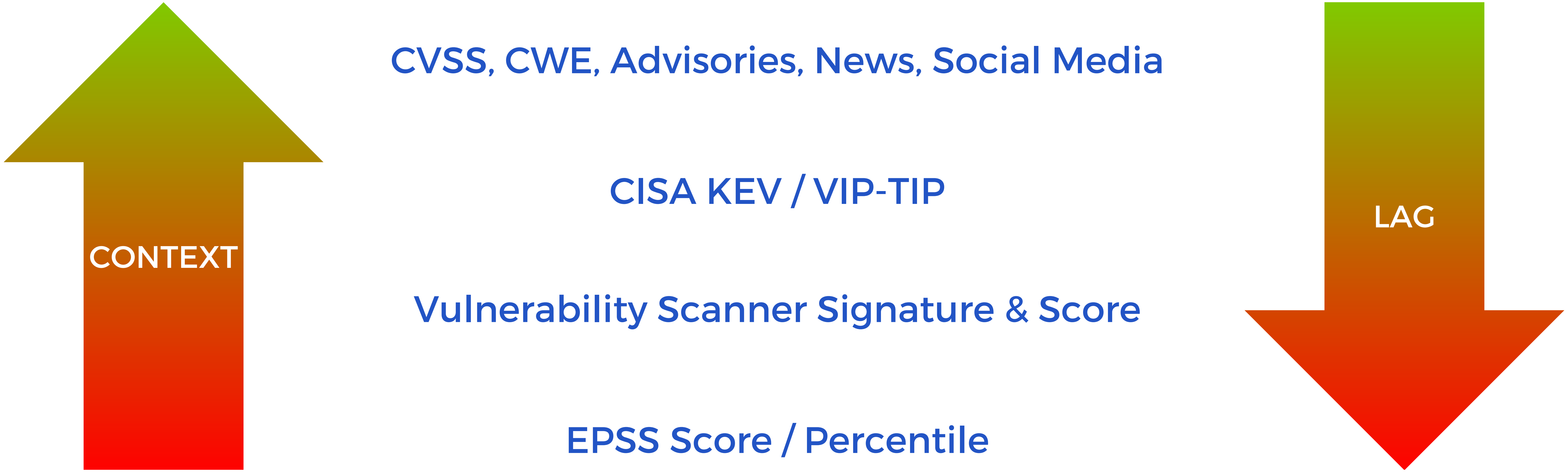
Policies, Procedures, Playbooks

Tabletop – Core Edge Device

Tabletop – 3rd Party Lib

Tabletop – Software

Prioritizing



CONTEXT

CVSS, CWE, Advisories, News, Social Media

CISA KEV / VIP-TIP

Vulnerability Scanner Signature & Score

EPSS Score / Percentile

LAG

Context is King

Is the vulnerability being actively exploited?

Is it used in ransomware or by APT groups?

Does it have publicly available POC’s?

Does it result in RCE? Code Injection? Authentication bypass?

Live Demo #2

Q & A

Get in Touch

Stay up to date with the latest research
Subscribe to our Vulnerability Intelligence Newsletter

raffi@vulnera.com

Follow us on LinkedIn