CVSS 3.1 vs. CVSS 4.0

Goods and Bads

Pete Allor and Nick Leali

Agenda

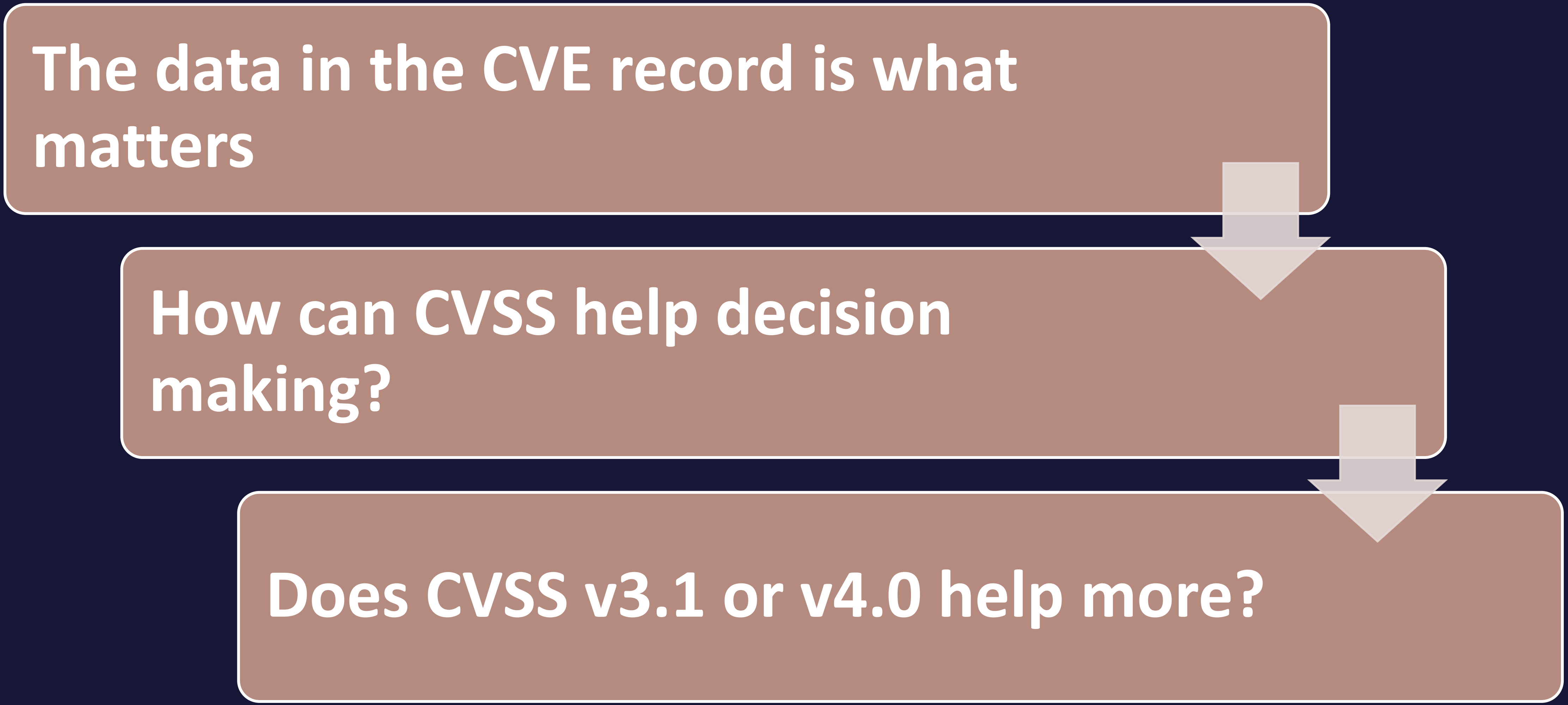
CVE is Meaningless

CVSS v3.1 Overview

CVSS v4.0 is Different

CVSS v3.1 / v4.0 Data Comparison

CVE is Meaningless



The data in the CVE record is what matters

How can CVSS help decision making?

Does CVSS v3.1 or v4.0 help more?

CVSS v3.1 Overview

Broadly Supported CVSS v3.1

A standard for a decade

Well-supported in tooling

Predictable math outcomes

CVSS v4.0 Is Different

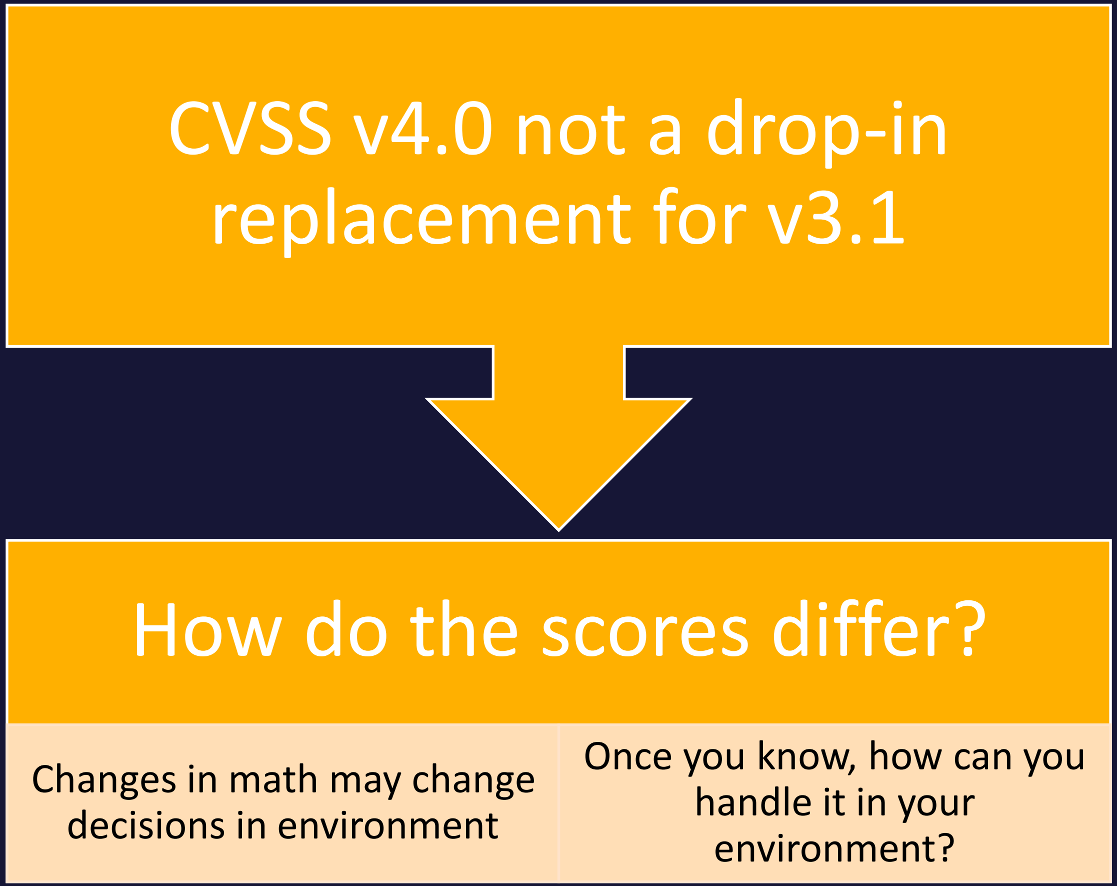
CVSS v4.0 New Features

- **Finer granularity, new Base metrics**
  - Vulnerable system impacts
  - Subsequent system impacts
- **New Math**
  - Outcome more balanced with Threat and Environmental
- **Supplemental Metrics**

- **Modified Base metric**
  - Attack Complexity (AC)
- **New Base metric**
  - Attack Requirements (AT)
- **New Base metric values**
  - User Interaction (UI): Passive (P) and Active (A)

This Is New Math

- Who is this for?
- Incident handlers
- Vendors who are considering CVSS v4.0 support
- CVSS consumers who want to start handling CVSS v4.0 vectors



CVSS v4.0 not a drop-in replacement for v3.1

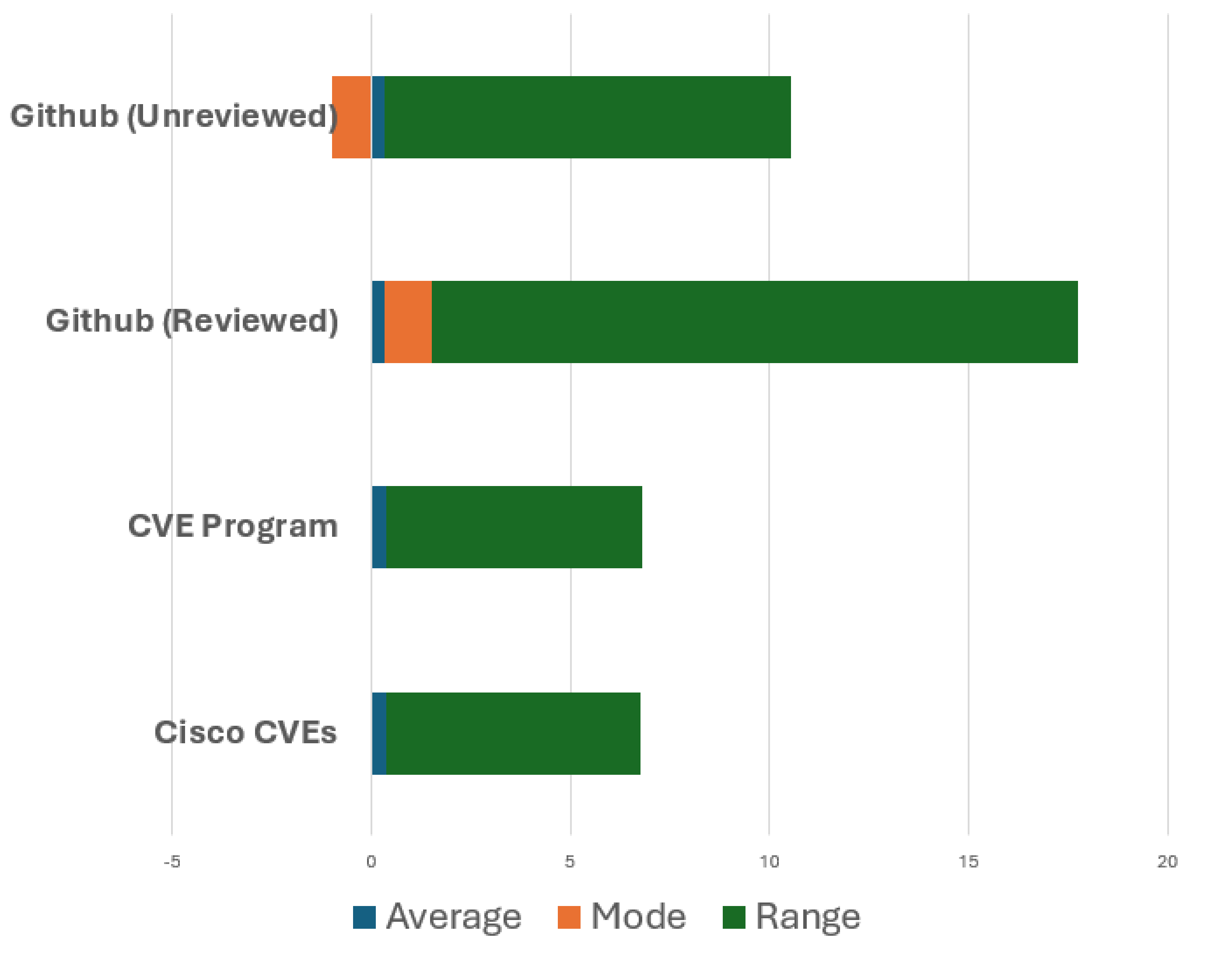
How do the scores differ?

Changes in math may change decisions in environment	Once you know, how can you handle it in your environment?

Comparing v3.1 to v4.0 in Data

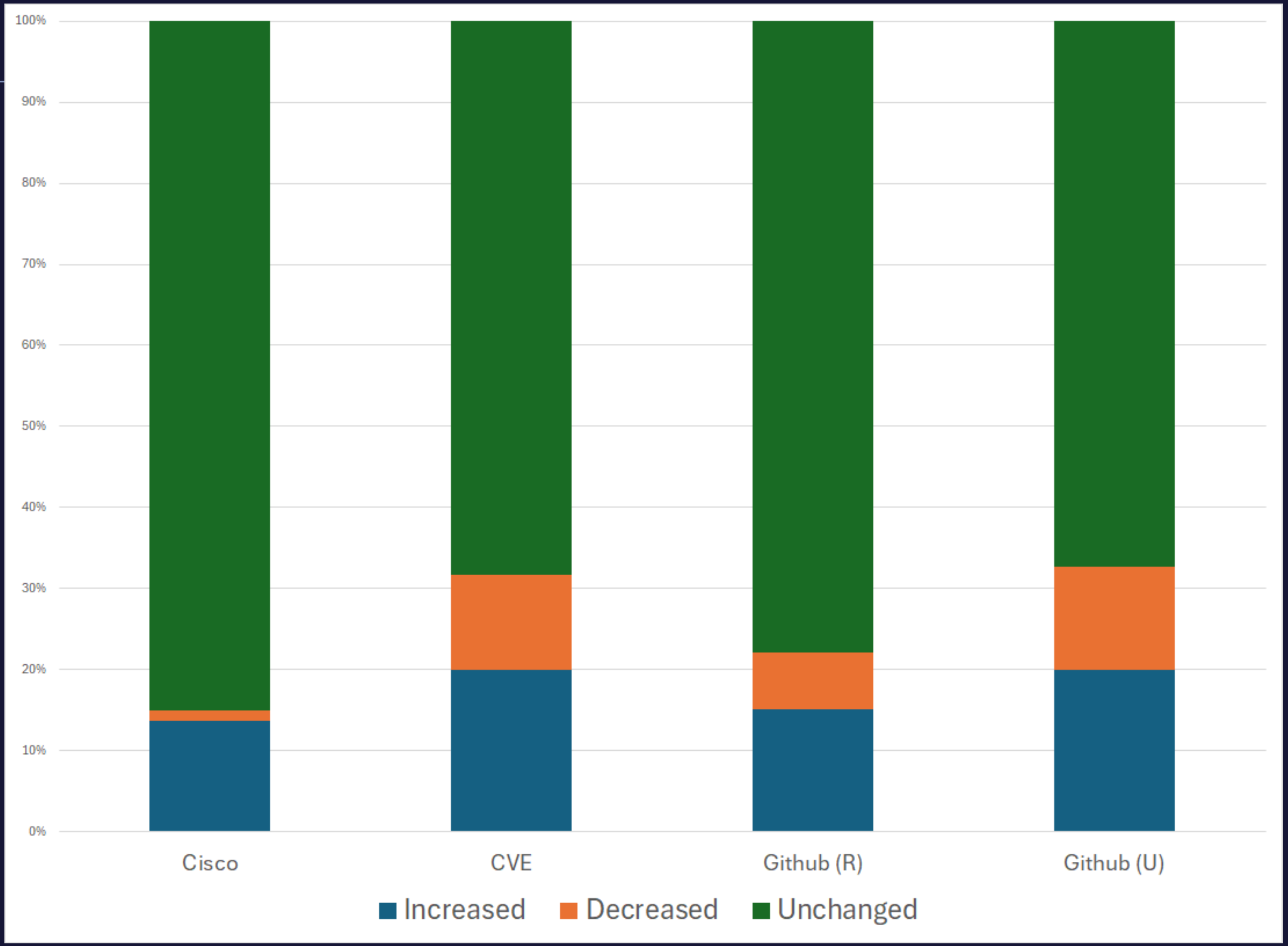
Changes in data sets

- Fairly limited overall changes
- Average changes small (less than 4%)
- Individually, big changes
- Ranges are wide, but likely error-prone



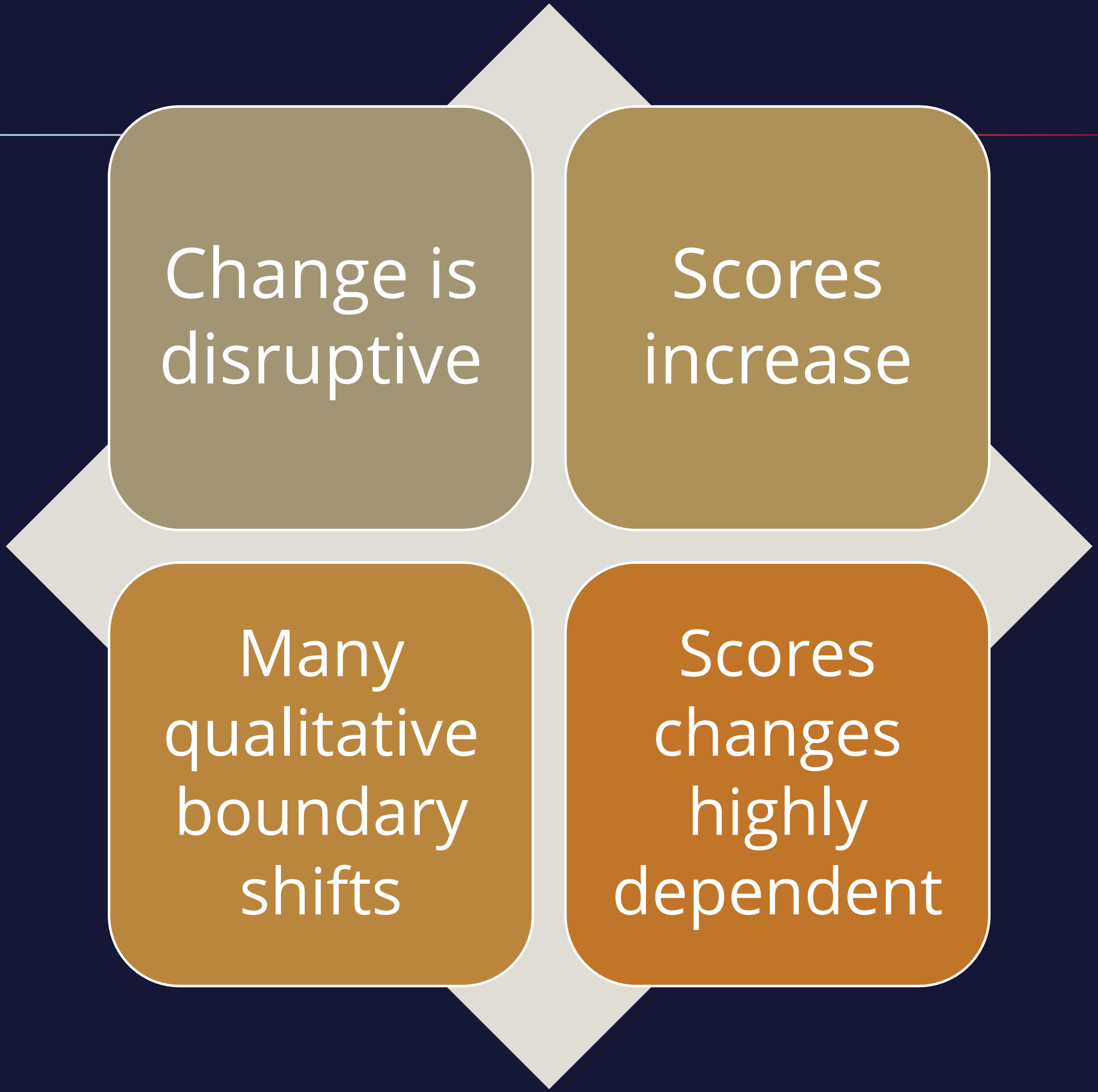
Boundary Changes

- Ratio of entire set
- Represents some big boundary shifts
- Ultimately impacts decision making!



Key Takeaways

CVSS v4.0 is Different



Change is disruptive

Scores increase

Many qualitative boundary shifts

Scores changes highly dependent

Improving CVSS Data Context

CNAs

- Careful of making promises solely on CVSS Base
- Look more to either full BTE or other identifiers
- Fall back to qualitative ratings
- Your own system, or CVSS Supplemental, or both!

CVE Consumers

- Careful using only CVSS Base for vulnerability management decisions
- Don’t rely on just CVSS
- Look at EPSS, SSVC, other systems
- Private systems such as Kenna or others

Q&A Time

CVE 25 YEARS

The mission of the CVE Program is to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered then assigned and published by organizations from around the world that have partnered with the CVE Program. Partners publish CVE Records to communicate consistent descriptions of vulnerabilities. Information technology and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities.

Learn more www.cve.org