Desperately Seeking Severity

Art Manion
amanion@cert.org
@zmanion

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-0411

About

Carnegie Mellon University

Software Engineering Institute (SEI)

- Federally Funded Research and Development Center (FFRDC)

CERT Coordination Center (CERT/CC)

- One of many Computer Security Incident Reponse Teams (CSIRTs)

Art Manion

- Technical Manager, Vulnerability Analysis Team
- CVSS contributor, member of FIRST and CVSS-SIG

I feel bad criticizing CVSS, really. But I'm trying to make it better.

CVSS identity crisis

Seeking: Information to make better risk decisions. Ideally free and from a reliable source.

Found: Proximate severity and impact of a vulnerability. With numbers!

Close enough.

A Brief History of CVSS

2004: CVSS v1

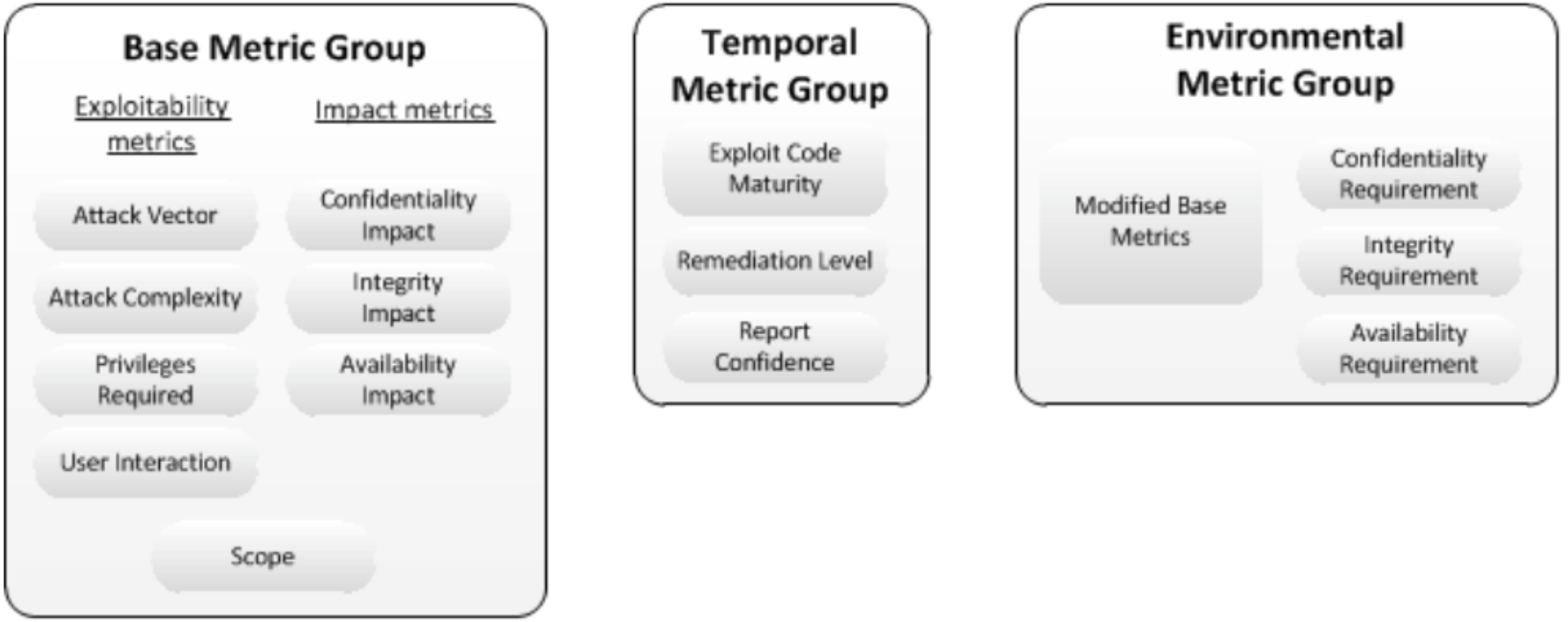
2005: National Infrastructure Advisory Council (NIAC) transitions ownership to Forum of Incident Response and Security Teams (FIRST)

2007: CVSS v2

2015: CVSS v3

Developers: Vulnerability scanner/management vendors, large commercial software vendors, vulnerability databases (NVD, CERT/CC, VulnDB)

CVSS metric groups



https://www.first.org/cvss/specification-document

Severity, priority, risk, and CVSS

Severity

- Intensity, degree, significance
- Vulnerability severity != risk severity

Priority

- Importance, precedence

Risk

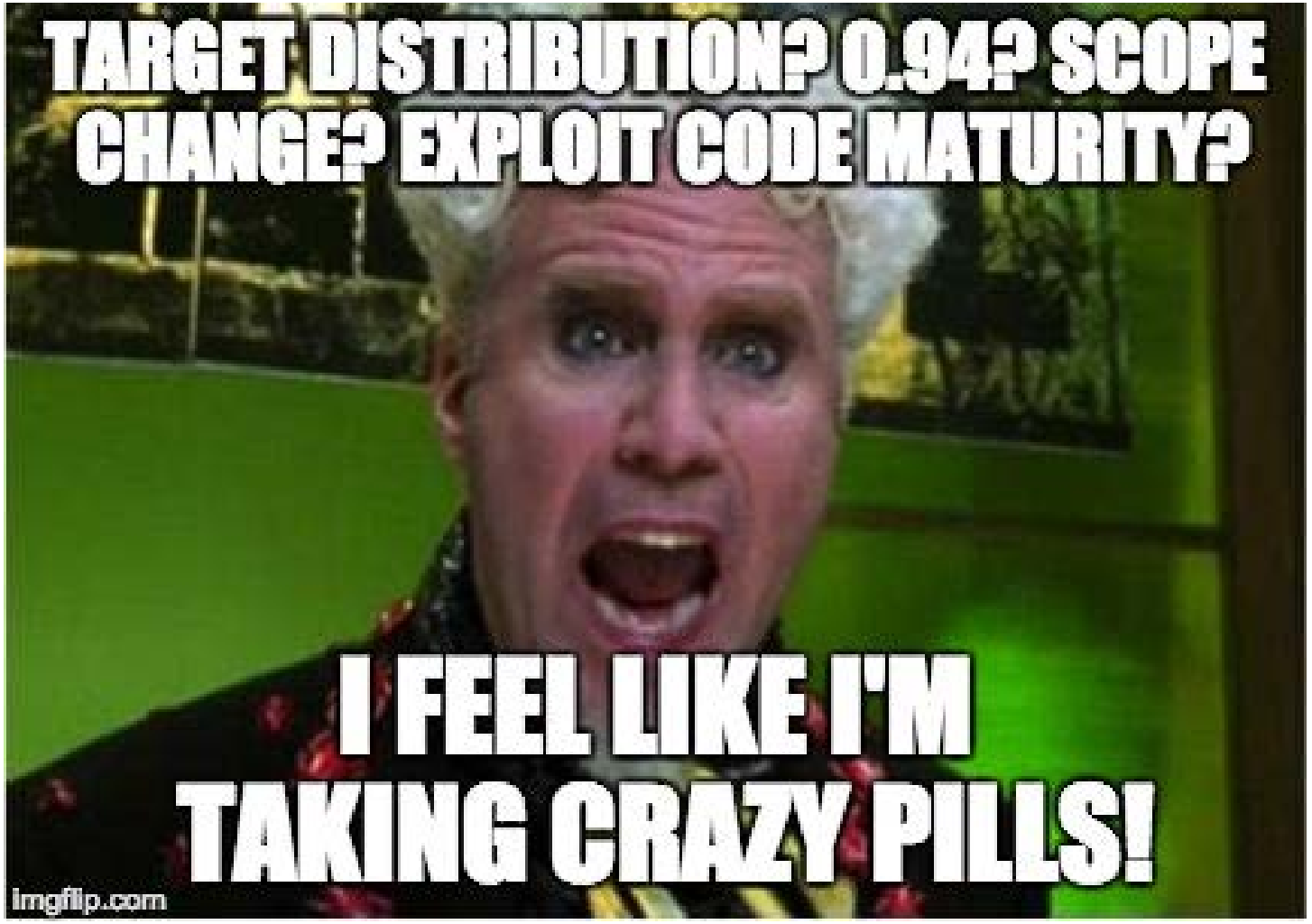
- Possibility of harm or loss

f(threat, vulnerability, loss)

Rank influence of terms in risk equation:

1. Loss ← CVSS Environmental (partial, v2 only)
2. Threat ← CVSS Temporal (broken)
3. Vulnerability ← CVSS Base (nearly irrelevant)

CVSS: Issues



CVSS: Issues

Target Distribution

- Significant environmental metric, gone in v3

Math

- Experts score and rank severity then create math to fit
- Exploit Code Maturity: Proof of Concept = 0.94
- Expected distribution?

Scope change (v3)

- Vulnerable component and the impacted component are different
  - VM escape, XSS
- v2 assumes OS is target
- Is scope change significant?

CVSS: Issues

Exploit Code Maturity

- High (worm) = 1.0
- Not Defined = 1.0
- Can't measure the difference between nearly every vulnerability and the handful that are known to be exploited
  - Exploit Intelligence Project presentation (Guido)
    https://www.nccgroup.trust/globalassets/resources/us/presentations/eip-final.pdf

Inability of CVSS to predict either attacks or lack of attacker interest

- Patching based on CVSS Base scores is a bad investment
  - Papers by Allodi and Massachi
    http://disi.unitn.it/~allodi/allodi-12-badgers.pdf

Difficulty accounting for exploit mitigations and differences across platforms

- v3 Environmental model might help

Example: CVE-2014-0160

Heartbleed!

CVSS v2 Base Score: 5.0

- Vector: (AV:N/AC:L/Au:N/C:P/I:N/A:N)

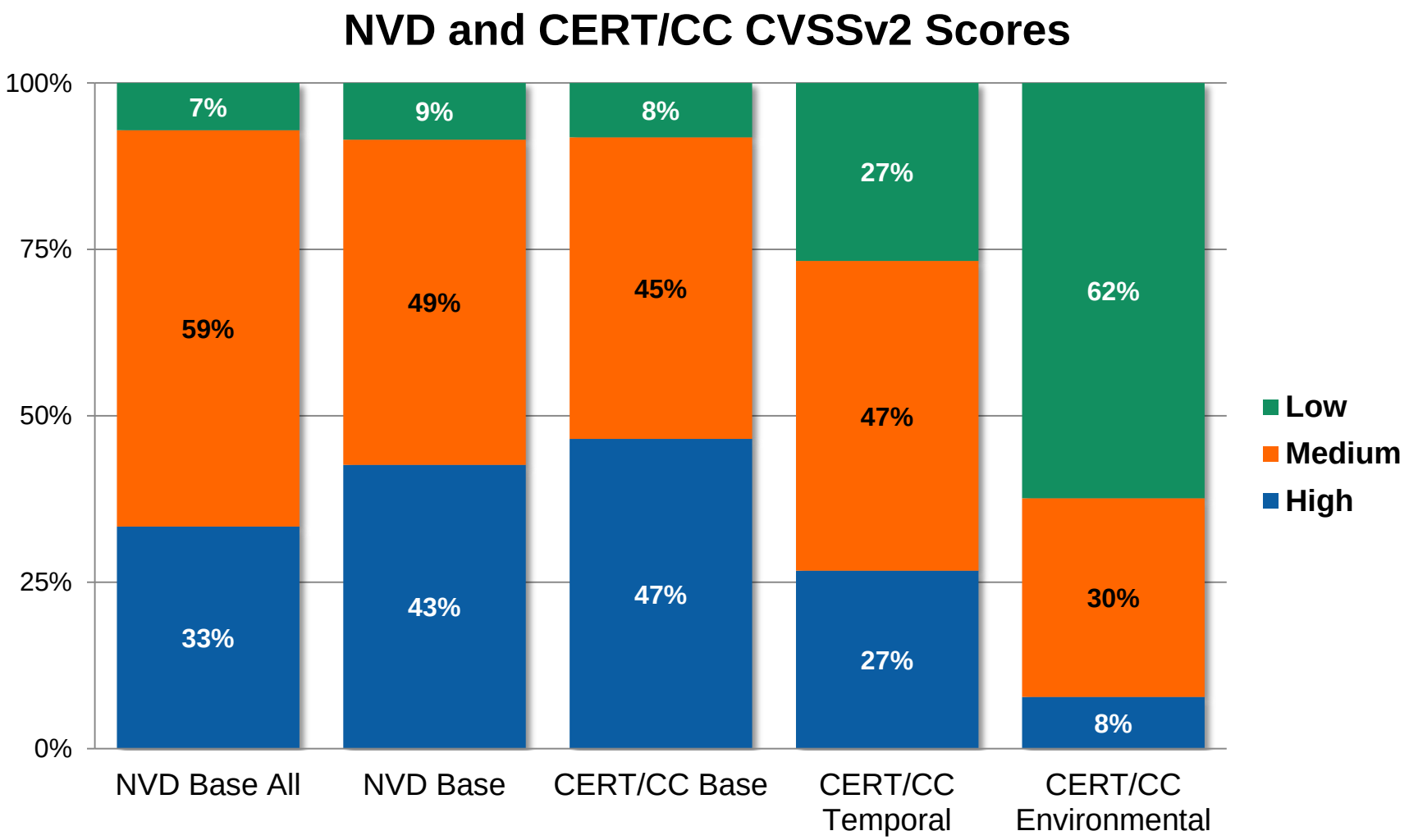
CVSS v2 Full Score: 6.4

- Vector: (…E:F/RL:OF/RC:C CDP:LM/TD:H/CR:H/IR:H/AR:ND)

CVSS v3 Base Score: 7.5

- Vector: (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

Full CVSS v2 scores



Vulnerability information for defense

What are you trying to do?

- Make better risk decisions

Am I going to get hit?

- Are other people being hit?

How bad will it be?

- Proximate vulnerability severity and impact are (much) less interesting than overall consequence
- CVSS Base won't help
  - Provides proximate vulnerability severity and impact

Challenges

Decision making with incomplete information

- Even “deep uncertainty” – Robust Decision Making (RDM)
- Volatility, uncertainty, complexity and ambiguity (VUCA)

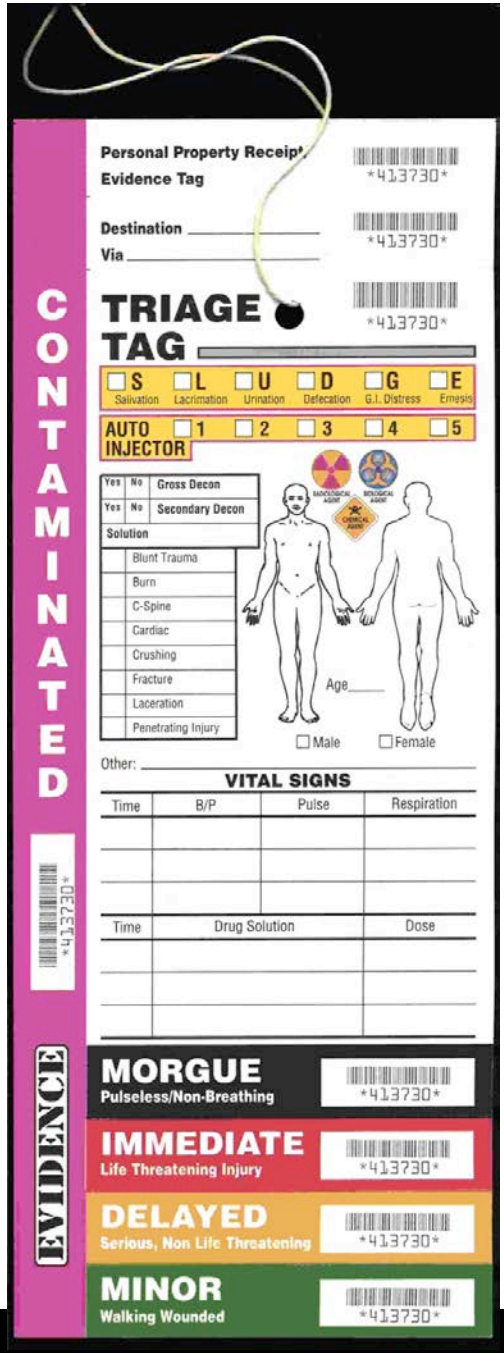
Ask smaller, more simple questions requiring less information

- Focus on threat and loss (context, environment)
- Avoid information that doesn’t contribute to the answers

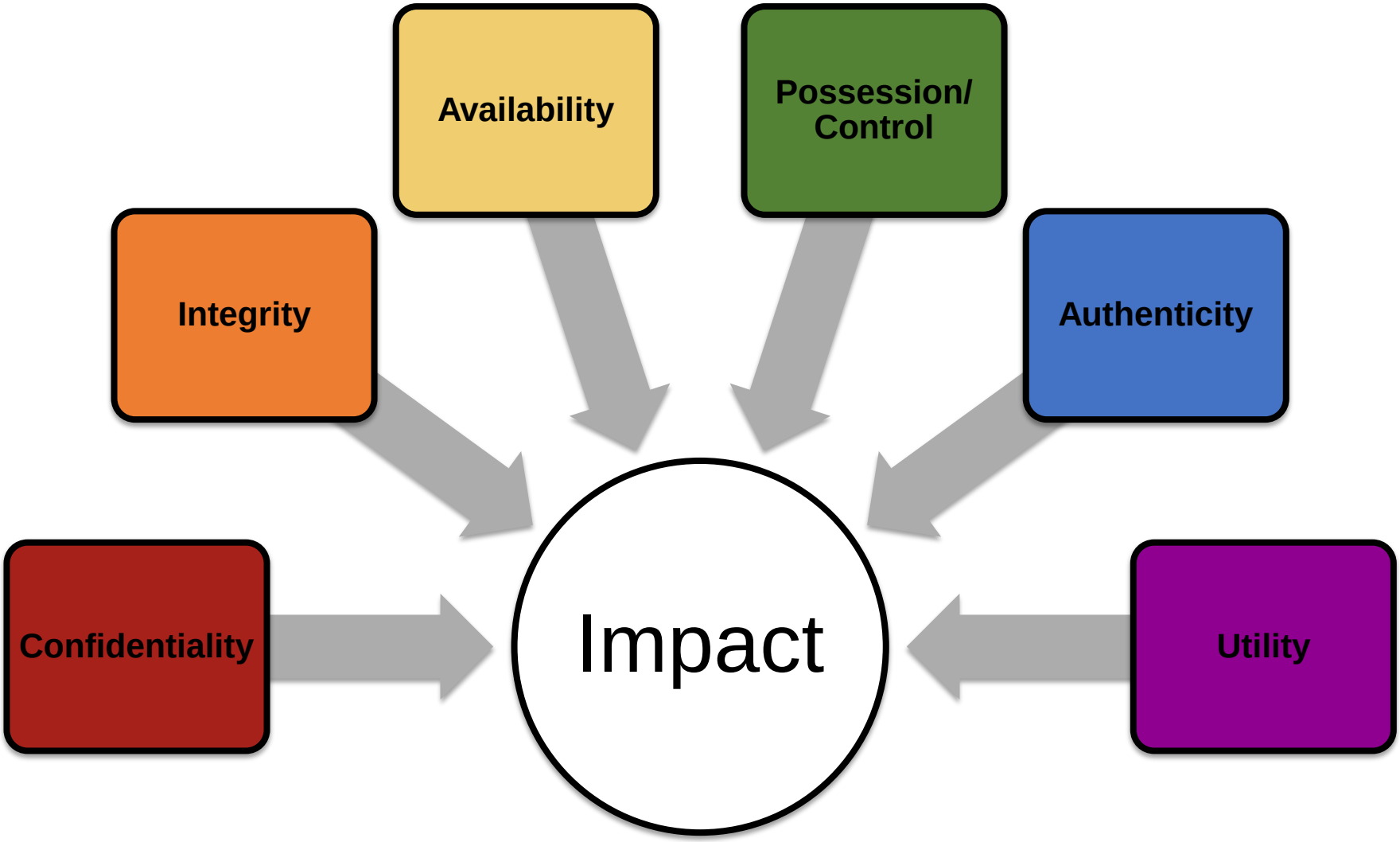
Triage

Quick initial assessment, classification, severity, prioritization

- Depending on results of triage, may perform additional assessment
  - Time and analysis effort can provide more information



Parkerian Hexad



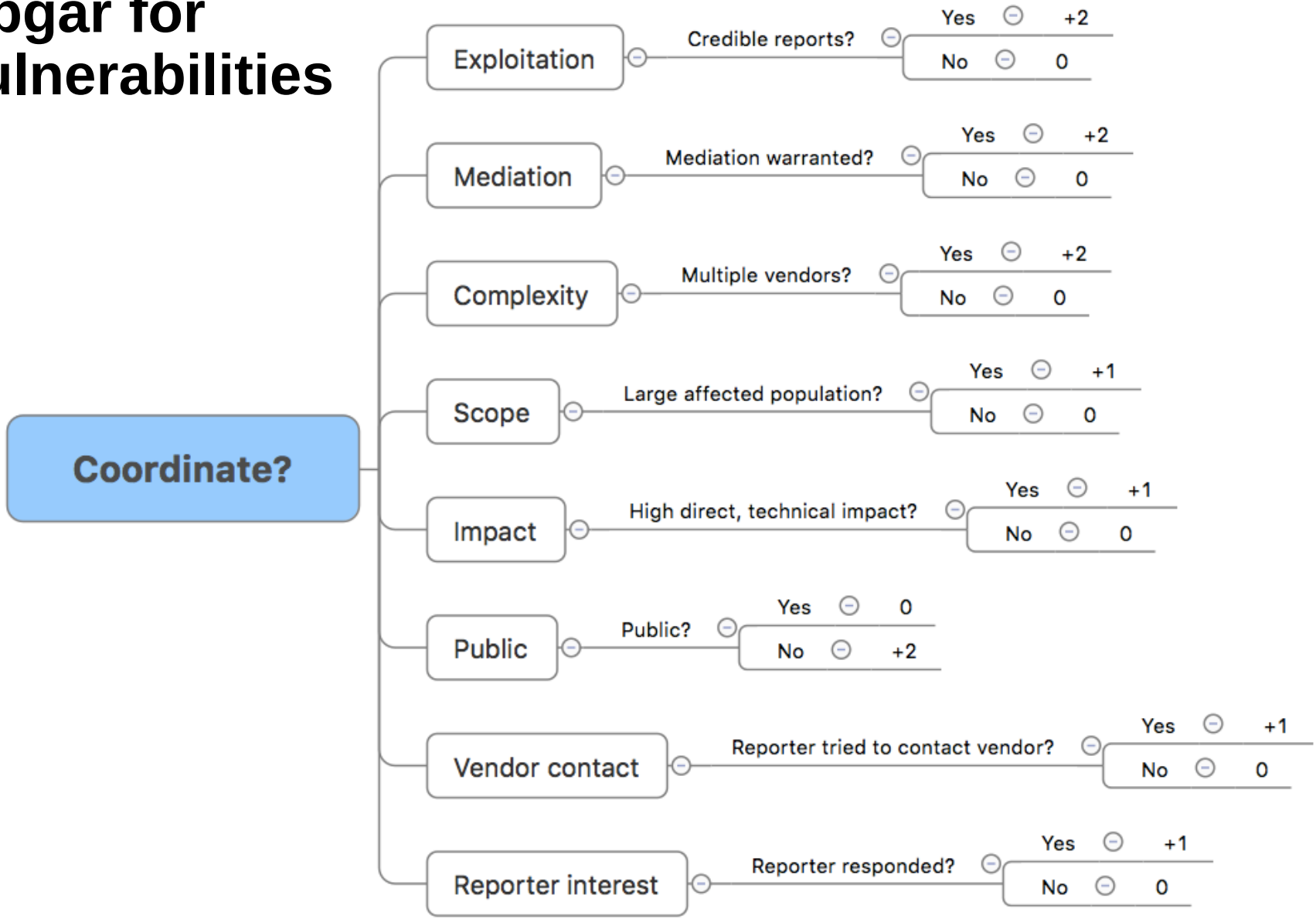
Apgar for babies

	0 (Points)	1	2
Appearance	Blue or pale all over	Blue extremities, but torso pink	Pink all over
Pulse	None	< 100	≥ 100
Grimace	No response	Weak grimace when stimulated	Cries or pulls away when stimulated
Activity	None	Some flexion of arms	Arms flexed, legs resist extension
Respirations	None	Weak, irregular or gasping	Strong cry

0-3 Critically Low, 4-6 Fairly Low, 7-10 Generally Normal

http://www.myheahenge.net/apgar-scoring-charts/

Apgar for vulnerabilities



Microsoft Exploitability Index

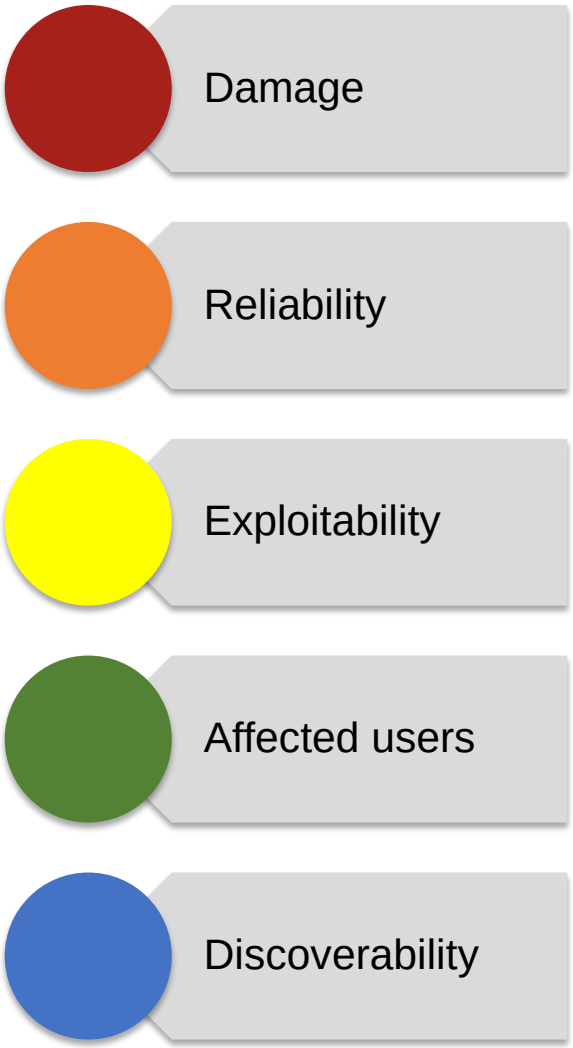
Exploitability Index Assessment	Short Definition
0	Exploitation Detected
1	Exploitation More Likely *
2	Exploitation Less Likely **
3	Exploitation Unlikely ***

"…prioritize security bulletin deployment by providing information on the likelihood that a vulnerability…will be exploited."

"…requests for additional information to further evaluate risk."

https://technet.microsoft.com/en-us/security/cc998259.aspx

DREAD



Examples:

- Severity = f(Da, R, A)
- Base severity (1-5) = Damage + f(R, A)
- If R + A > 4 add 2
  else if R + A > 3 add 1
  else add 0

"This is NOT how MSRC does things.… Warning! Do NOT apply this system, or any other system, without THINKING about it."

- David LeBlanc, Microsoft (2007)

"We tried many math models before we realized that math was the problem. We were trying to assume relationships based on data that had no relationship."

- Keith Maxon

https://blogs.msdn.microsoft.com/david_leblanc/2007/08/14/dreadful/

Bugcrowd's Vulnerability Rating Taxonomy

PRIORITY ▼	OWASP TOP TEN + BUGCROWD EXTRAS	SPECIFIC VULNERABILITY NAME	VARIANT OR AFFECTED FUNCTION
P1	Server Security Misconfiguration	Using Default Credentials	Production Server
P2	Cross-Site Scripting (XSS)	Stored	Non-Admin to Anyone
P3	Server-Side Injection	HTTP Response Manipulation	Response Splitting (CRLF)
P4	Server Security Misconfiguration	Missing Secure or HTTPOnly Cookie Flag	Session Token
P5	Server Security Misconfiguration	Mail Server Misconfiguration	Missing SPF on Non-Email Domain

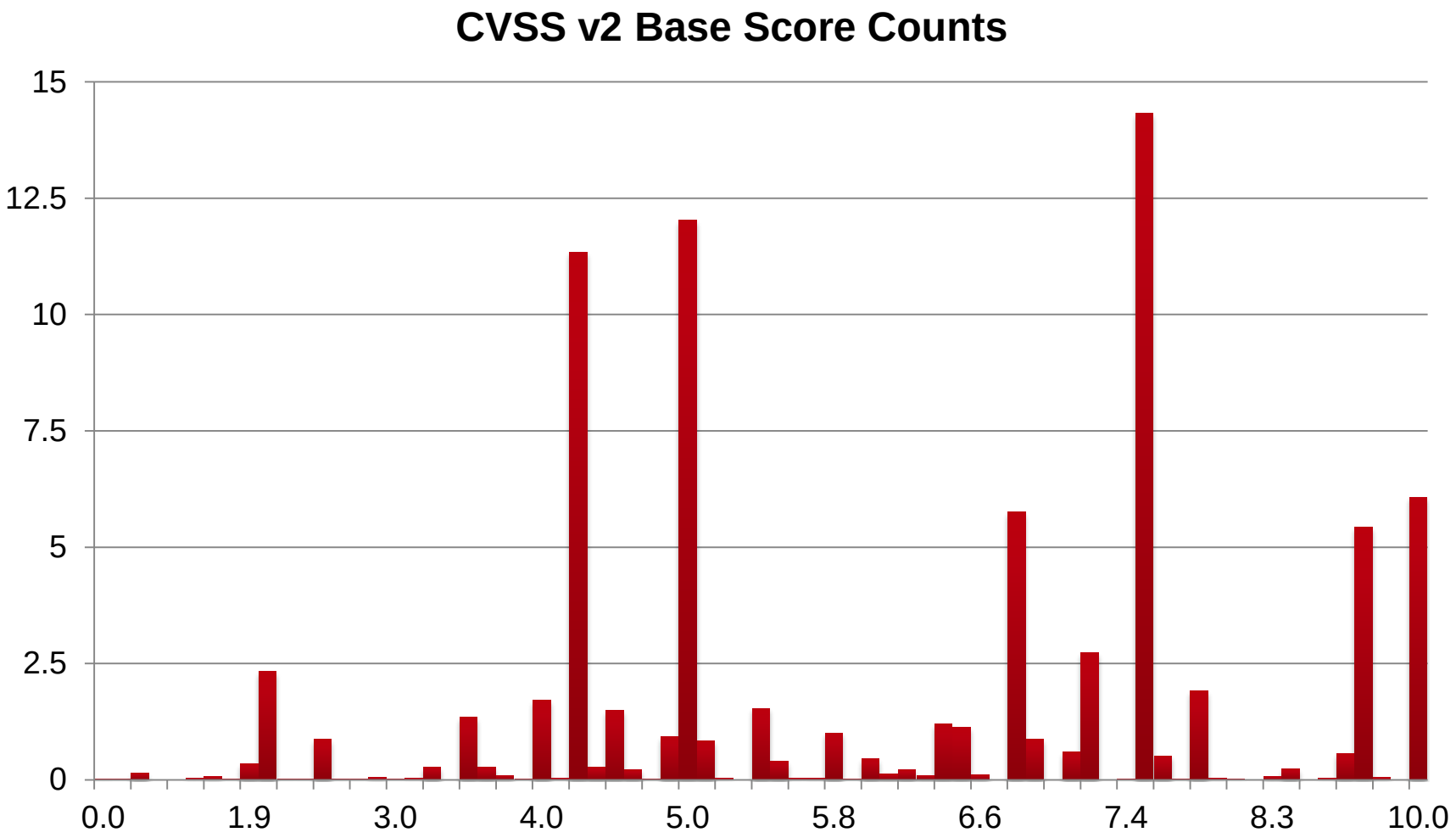
https://bugcrowd.com/vulnerability-rating-taxonomy

Vulnerability Response Decision Assistance (VRDA)

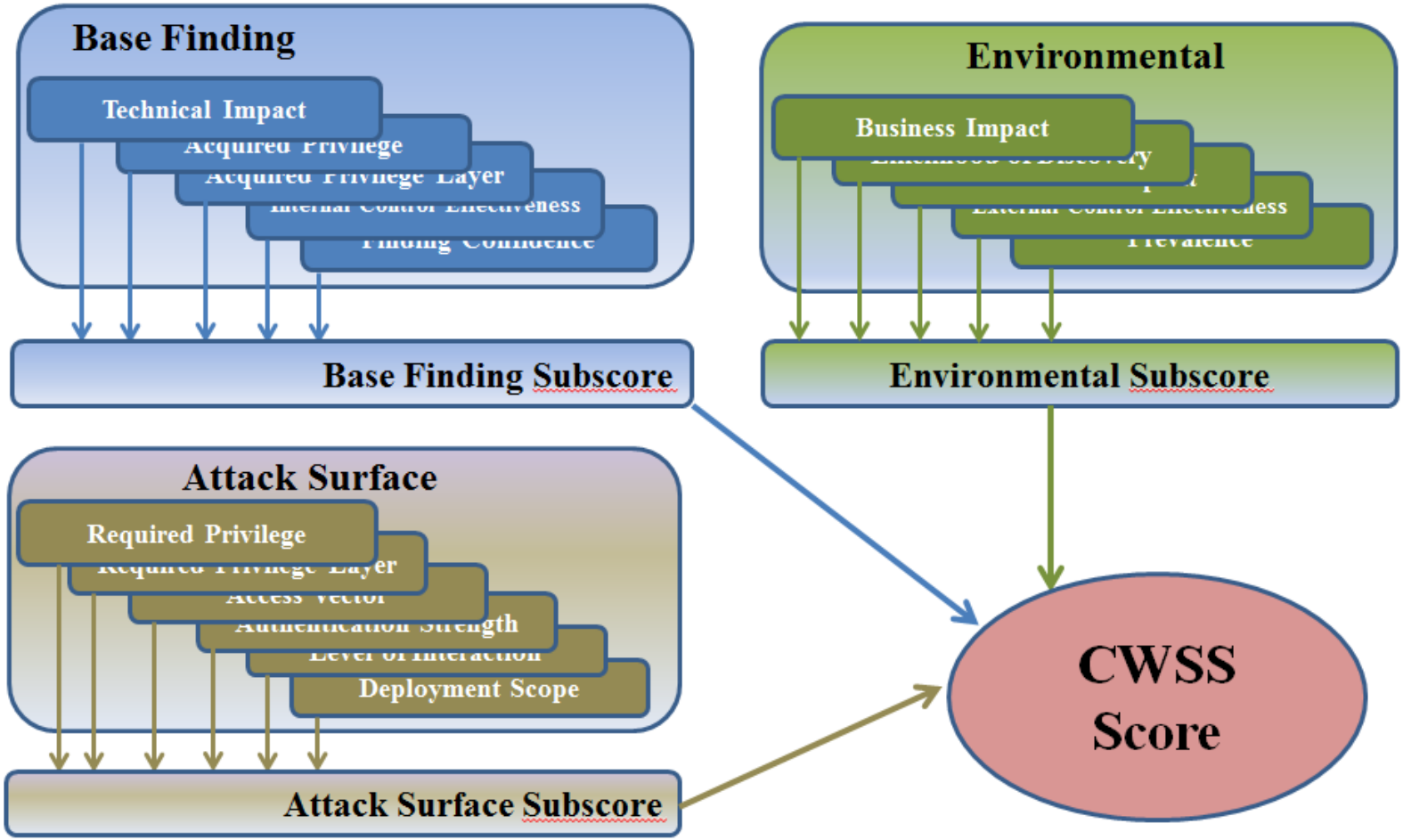
Task	Error						
	-3	-2	-1	0	1	2	3
Overall Performance (all tasks)	*4*	*40*	*256*	*1,500*	*264*	*52*	*31*
Assign Analyst (D1)			6	193	16		
Perform Surface Analysis	2	1	3	190	1	2	16
Perform Technical Analysis		3	39	146	16	9	2
Coordinate		4	44	125	32	7	3
Publish Vulnerability Card		2	27	147	31	6	2
Publish Vulnerability Note		2	28	141	33	9	2
Publish Technical Alert	1	9	27	129	36	10	3
Publish Security Alert	1	10	26	135	36	6	1
Publish Special Communication				173	40		2
Publish Current Activity		9	56	121	23	3	
			Design goal (NMR)				

http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=50301

CVSS vector combinations only, no math

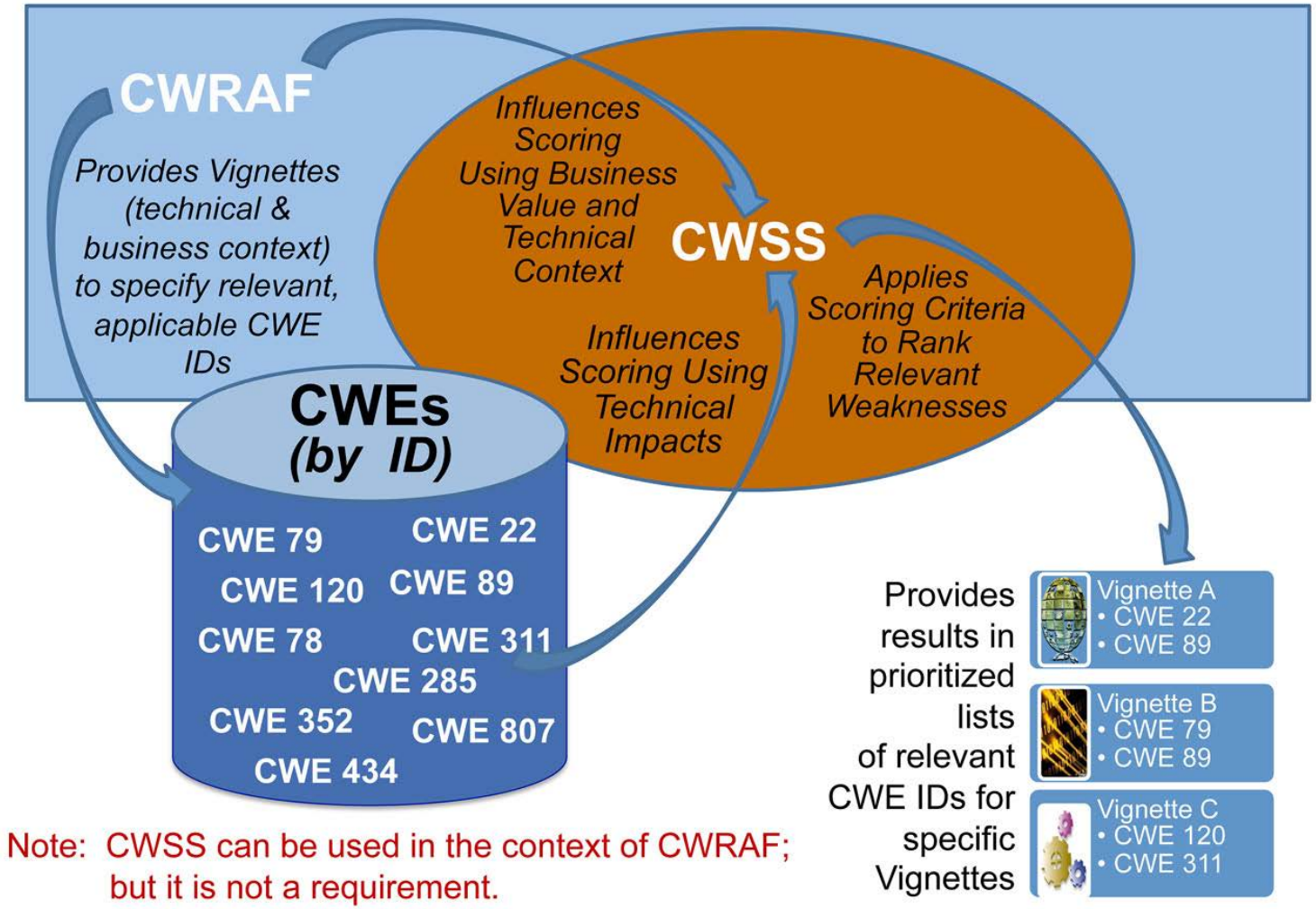


Common Weakness Scoring System (CWSS)



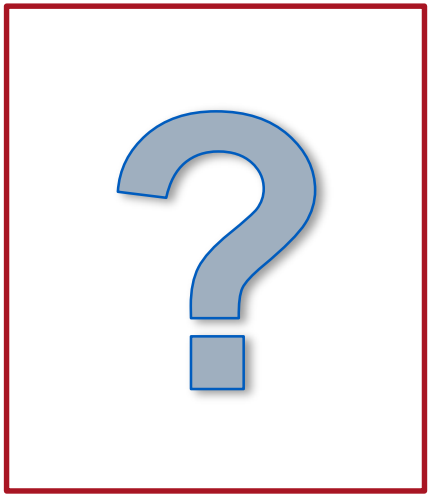
https://cwe.mitre.org/cwss/cwss_v1.0.1.html

Common Weakness Risk Analysis Framework (CWRAF)



https://cwe.mitre.org/cwraf/introduction.html

Questions



amanion@cert.org

@zmanion