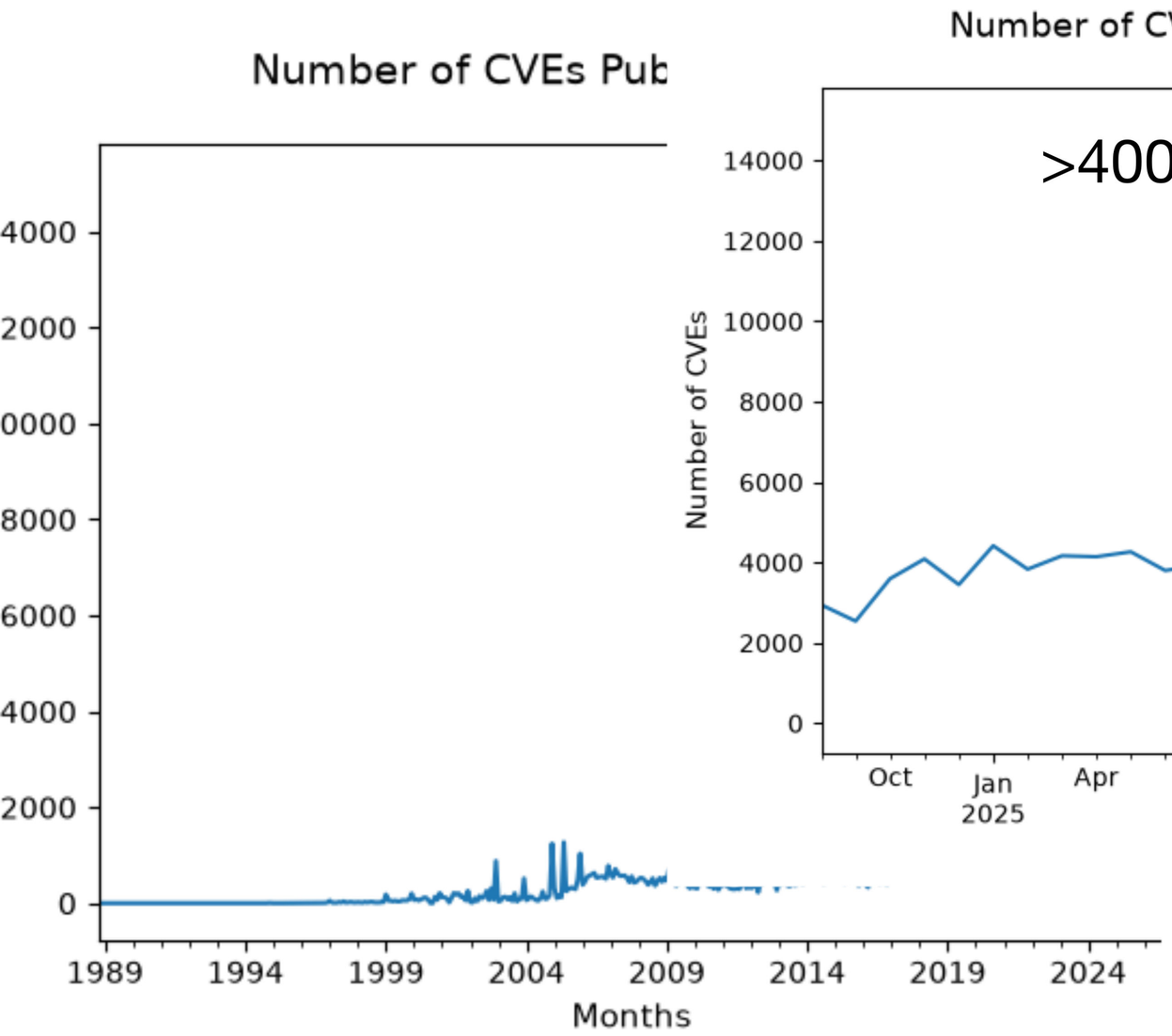
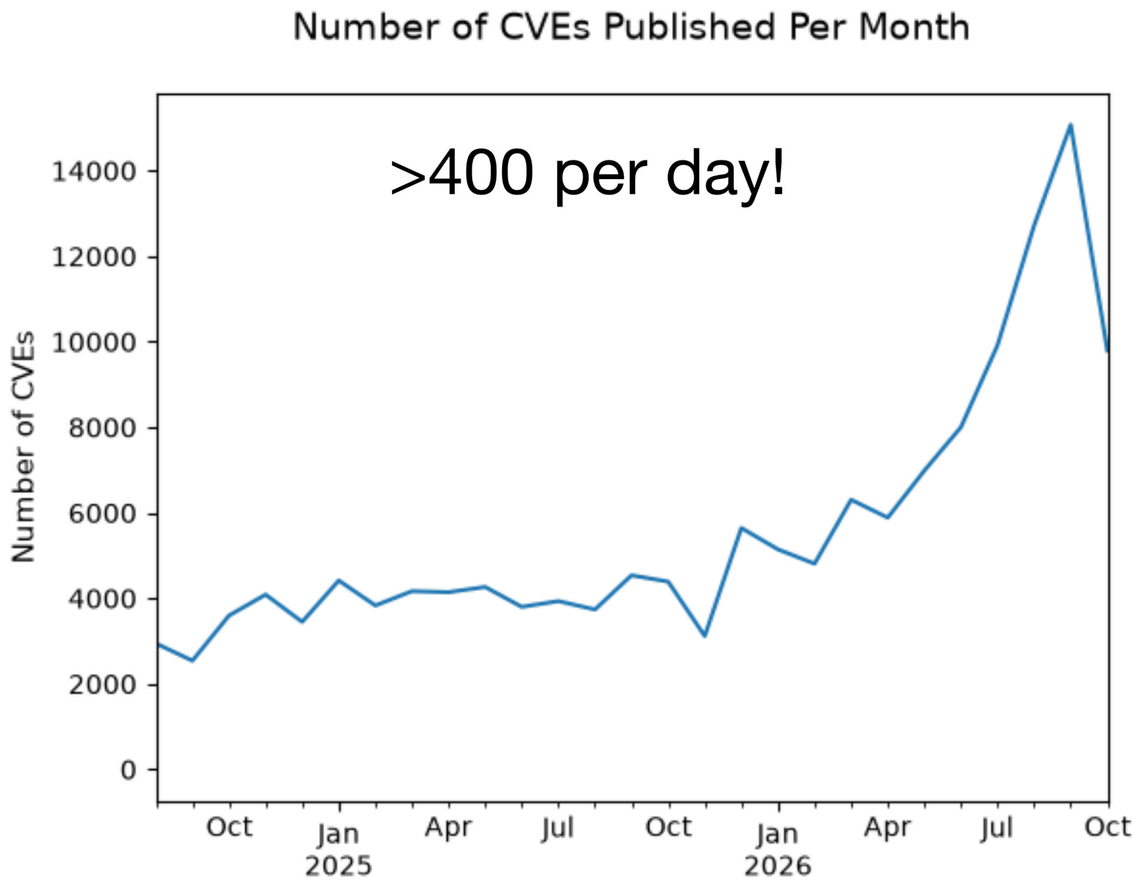
VULNERABILITY MANAGEMENT IN THE AGE OF AI

DR. JEROEN VAN DER HAM-DE VOS

UNIVERSITY
OF TWENTE.

Exploding CVEs





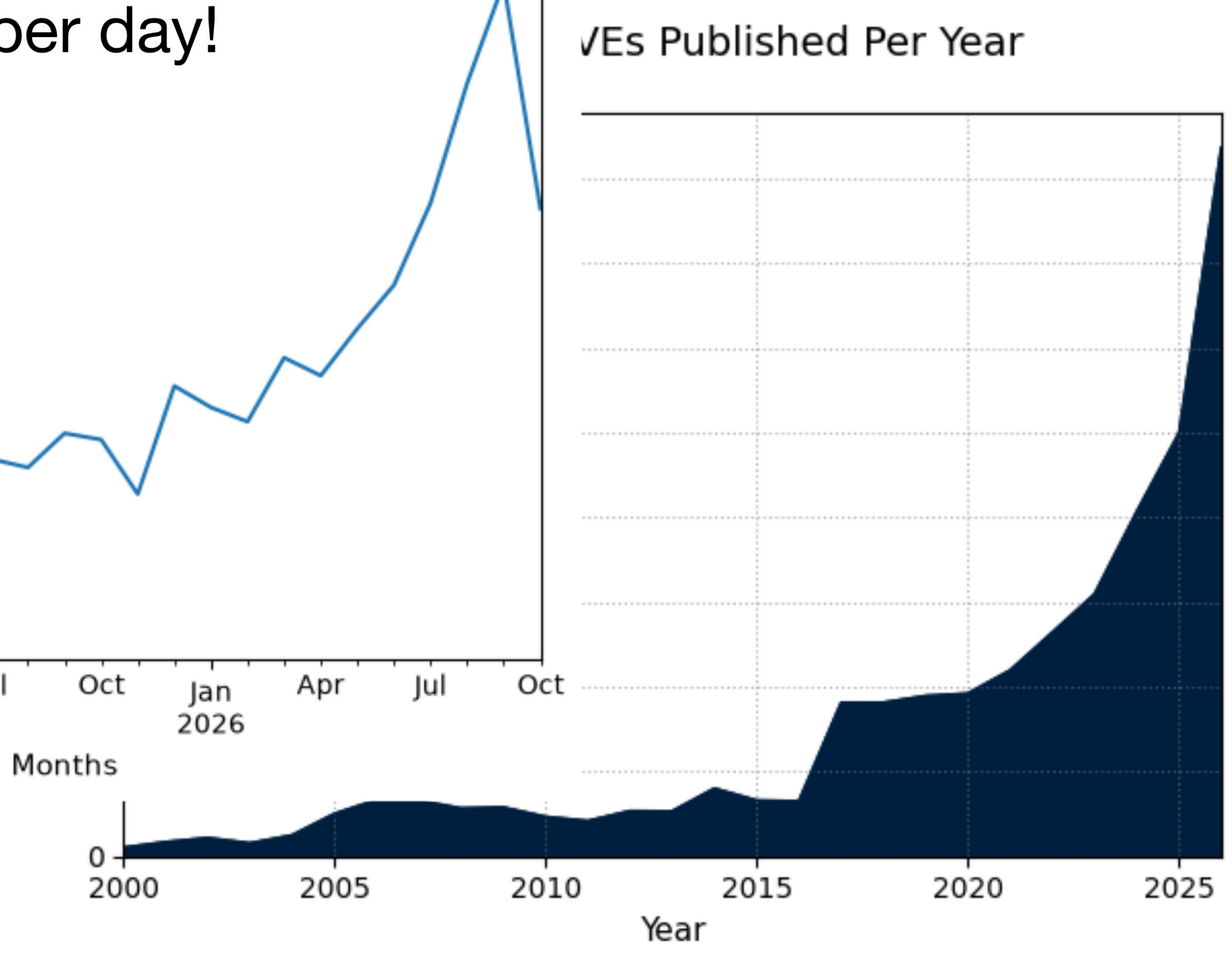


Photo by Rio Hodges on Unsplash

Photo by Rio Hodges on Unsplash

Who am I?

- Studied AI long before LLMs
- Studied networking before deep-sea cable cutting
- Now studying vulnerability management

  - International expert on CVD
  - Contributed to CVSS
  - CNA Admin at DIVD.nl

HOME > TECH > SECURITY

UniFi CVSS 10.0 Flaw Exposes 100,000 E
Unauthenticated Takeover

Prior UniFi OS chain is already under botnet attack; today adds unauthenticate

Cybercriminals Take Advantage of CVSS 10.0 Bricksforge Vulnerability in WordPress, Allowing Unauthenticated Remote Code Execution

*Last updated on **October 14, 2026** by **Souvik Banerjee** on **WordPress, Programming***

Home » News » WordPress » Cybercriminals Take Advantage of CVSS 10.0 Bricksforge Vulnerability in WordPress, Allowing Unauthenticated Remote Code Execution

The Hacker News

Get the Latest News

Home Vulnerabilities Cyber Attacks Expert Insights Awards

GitLab Patches CVSS 10.0 Flaw That Could Let Unauthenticated Users Run Server Code

Ravie Lakshmanan Oct 13, 2026 Vulnerability / DevSecOps

Runtime

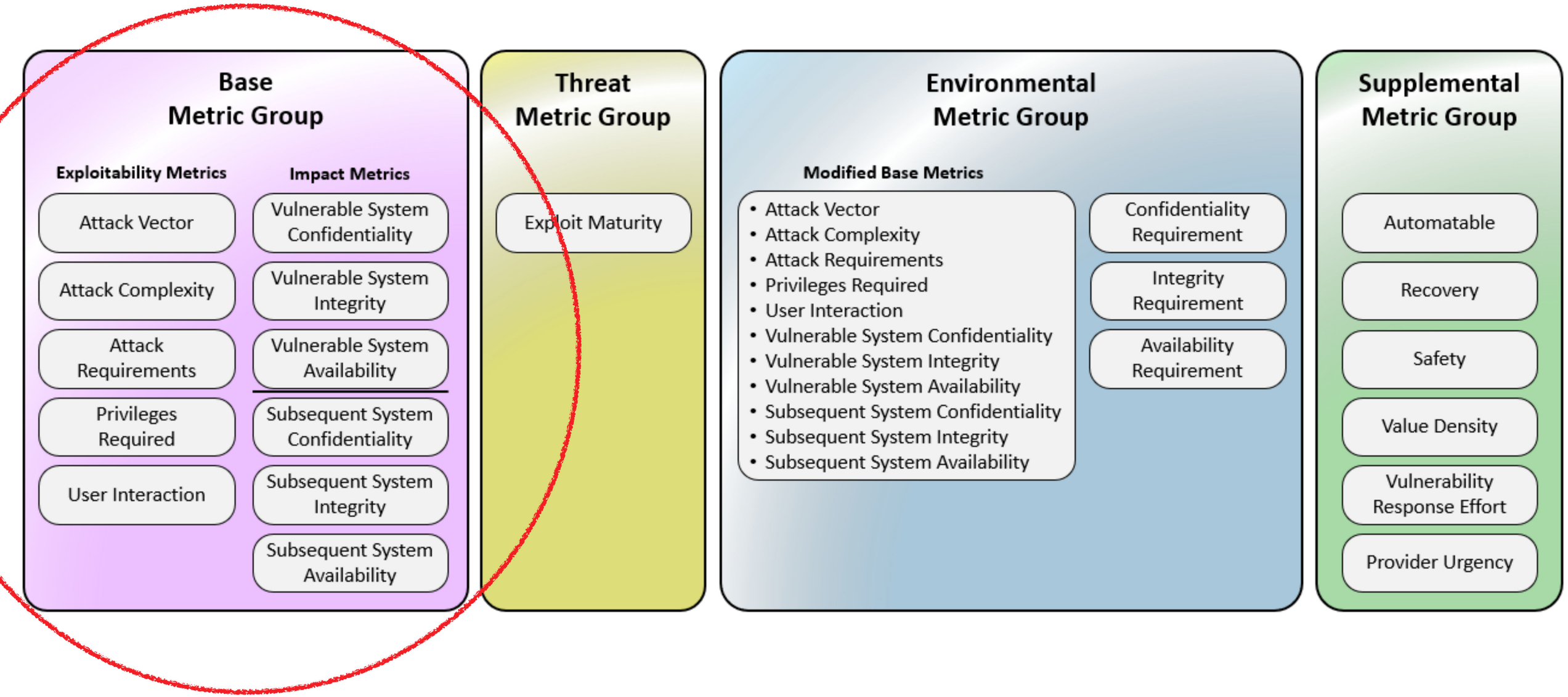
Runtime: SAP's kernel has a CVSS 10-shaped hole in it. Buckle up.

+ OpenAI's "observability" headaches, and more.

By Edward Targett

Updated Sep 8, 2026 5:17 PM / Published Sep 8, 2026 2:56 PM · 5 min read

CVSS v4.0


Base
Metric Group
Exploitability Metrics
Attack Vector
Attack Complexity
Attack Requirements
Privileges Required
User Interaction
Impact Metrics
Vulnerable System Confidentiality
Vulnerable System Integrity
Vulnerable System Availability
Subsequent System Confidentiality
Subsequent System Integrity
Subsequent System Availability
Threat
Metric Group
Exploit Maturity
Environmental
Metric Group
Modified Base Metrics
• Attack Vector
• Attack Complexity
• Attack Requirements
• Privileges Required
• User Interaction
• Vulnerable System Confidentiality
• Vulnerable System Integrity
• Vulnerable System Availability
• Subsequent System Confidentiality
• Subsequent System Integrity
• Subsequent System Availability
Confidentiality Requirement
Integrity Requirement
Availability Requirement
Supplemental
Metric Group
Automatable
Recovery
Safety
Value Density
Vulnerability Response Effort
Provider Urgency

https://www.first.org/cvss/v3-1/specification-document

ISS = **1 - [(1 - Confidentiality) × (1 - Integrity) × (1 - Availability)]**

Impact

If Scope

If Scope

Exploita

BaseSc

If Impac

If Scope

If Scope

UNIVERSITY OF TWENTE.

Photo by Elena Mozhvilo on Unsplash

CVSS vs Risk – RTFM

2.2. CVSS Base Score (CVSS-B) Measures Severity, not Risk

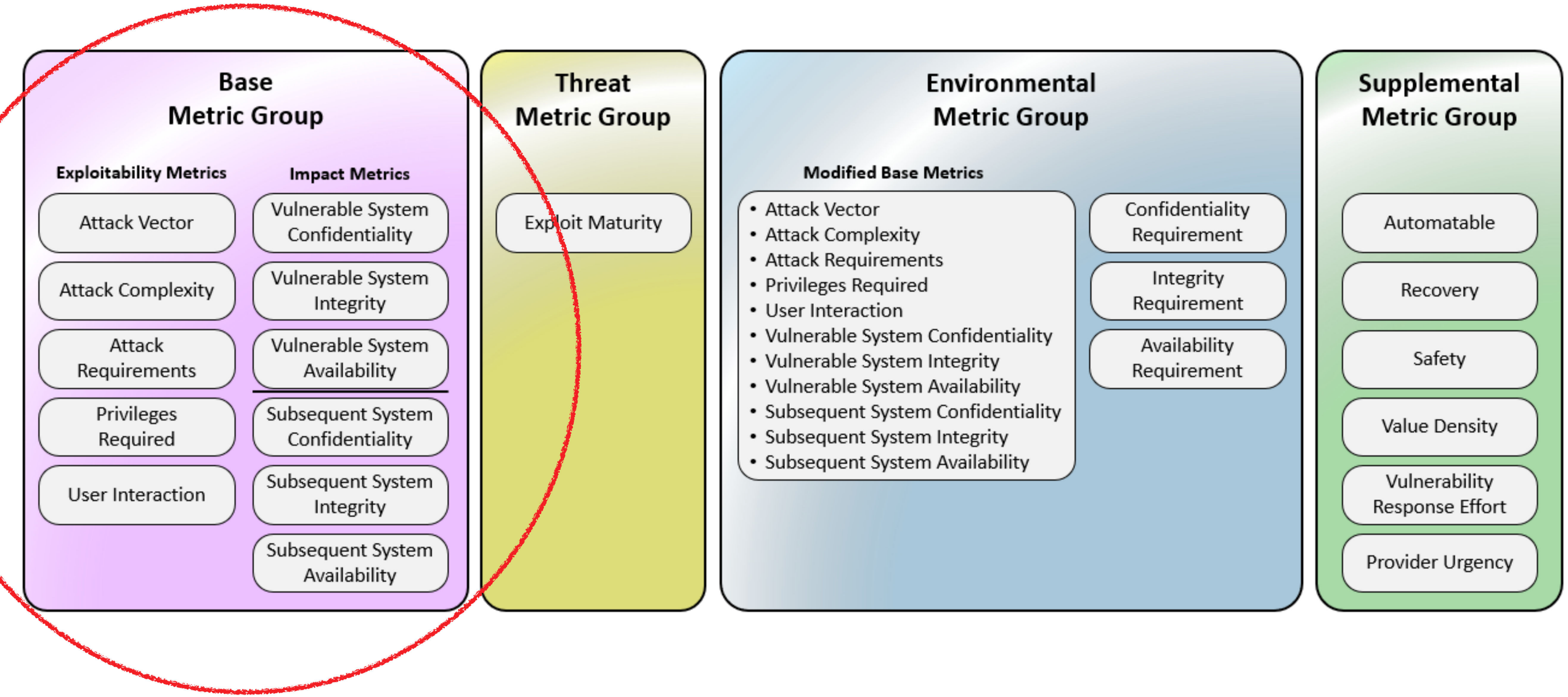
The CVSS Specification Document has been updated to emphasize and clarify the fact that CVSS Base (CVSS-B) scores are designed to measure the severity of a vulnerability and should not be used alone to assess risk.

The CVSS v4.0 Specification Document clearly states that the CVSS Base Score represents only the intrinsic characteristics of a vulnerability and is independent of any factor associated with threat or the computing environment where the vulnerable system resides.

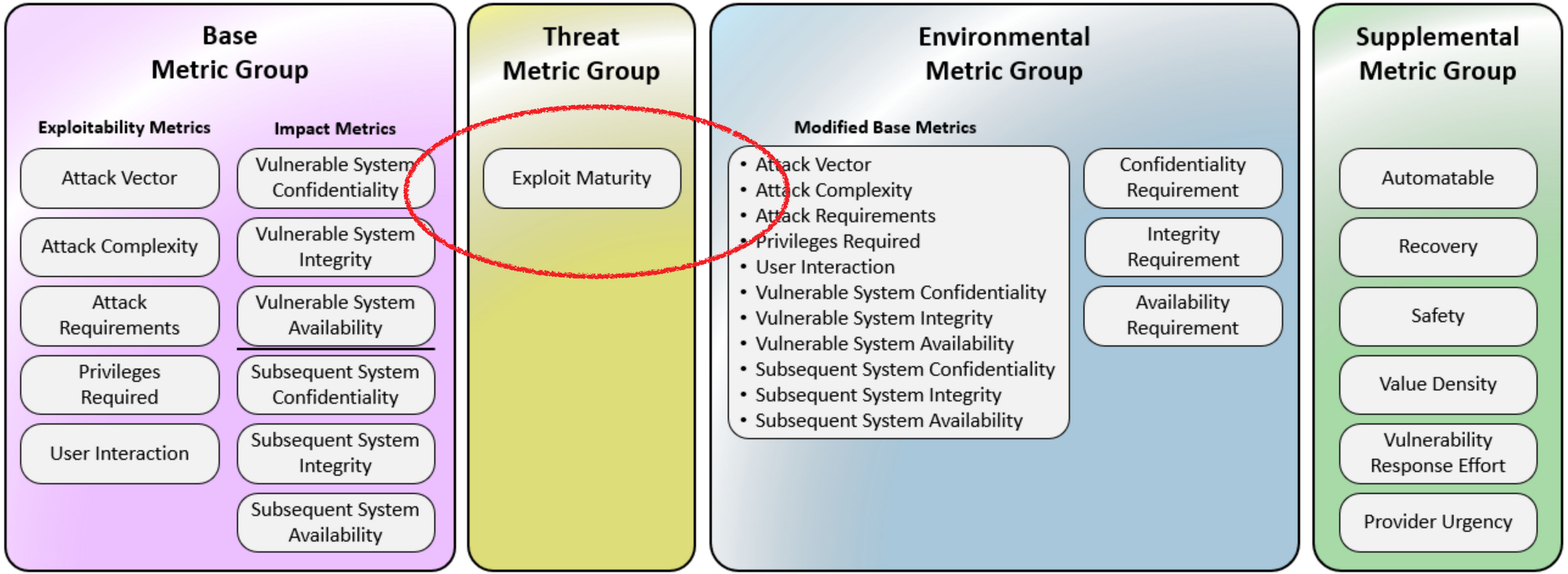
The CVSS Base Score should be supplemented with an analysis of the environment (Environmental Metrics), and with attributes that may change over time (Threat Metrics).

For an organization that employs automated methods to comprehensively utilize the Environmental and Threat metric groups, the resulting CVSS-BTE score can be considered much closer to “Risk”.

CVSS v4.0


Base
Metric Group
Exploitability Metrics
Attack Vector
Attack Complexity
Attack Requirements
Privileges Required
User Interaction
Impact Metrics
Vulnerable System Confidentiality
Vulnerable System Integrity
Vulnerable System Availability
Subsequent System Confidentiality
Subsequent System Integrity
Subsequent System Availability
Threat
Metric Group
Exploit Maturity
Environmental
Metric Group
Modified Base Metrics
• Attack Vector
• Attack Complexity
• Attack Requirements
• Privileges Required
• User Interaction
• Vulnerable System Confidentiality
• Vulnerable System Integrity
• Vulnerable System Availability
• Subsequent System Confidentiality
• Subsequent System Integrity
• Subsequent System Availability
Confidentiality Requirement
Integrity Requirement
Availability Requirement
Supplemental
Metric Group
Automatable
Recovery
Safety
Value Density
Vulnerability Response Effort
Provider Urgency

CVSS v4.0


Base
Metric Group
Exploitability Metrics
Attack Vector
Attack Complexity
Attack Requirements
Privileges Required
User Interaction
Impact Metrics
Vulnerable System Confidentiality
Vulnerable System Integrity
Vulnerable System Availability
Subsequent System Confidentiality
Subsequent System Integrity
Subsequent System Availability
Threat
Metric Group
Exploit Maturity
Environmental
Metric Group
Modified Base Metrics
• Attack Vector
• Attack Complexity
• Attack Requirements
• Privileges Required
• User Interaction
• Vulnerable System Confidentiality
• Vulnerable System Integrity
• Vulnerable System Availability
• Subsequent System Confidentiality
• Subsequent System Integrity
• Subsequent System Availability
Confidentiality Requirement
Integrity Requirement
Availability Requirement
Supplemental
Metric Group
Automatable
Recovery
Safety
Value Density
Vulnerability Response Effort
Provider Urgency

Reducing the Significant Risk of Known Exploited Vulnerabilities

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild: the Known Exploited Vulnerability (KEV) catalog. CISA strongly recommends all organizations review and monitor the KEV catalog and prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors.

America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Search

Topics | Spotlight | Resources & Tools | News & Events | Careers | About

Home / Known Exploited Vulnerabilities Catalog

Search all Known Exploited Vulnerabilities Catalog

Known Exploited

Showing 1 to 2 of 2 results

ZAMMAD GMBH | ZAMMAD

CVE-2026-1

Za *GmbH Zammad contains an improper* *ate privileges to root. This vulnerability can be*

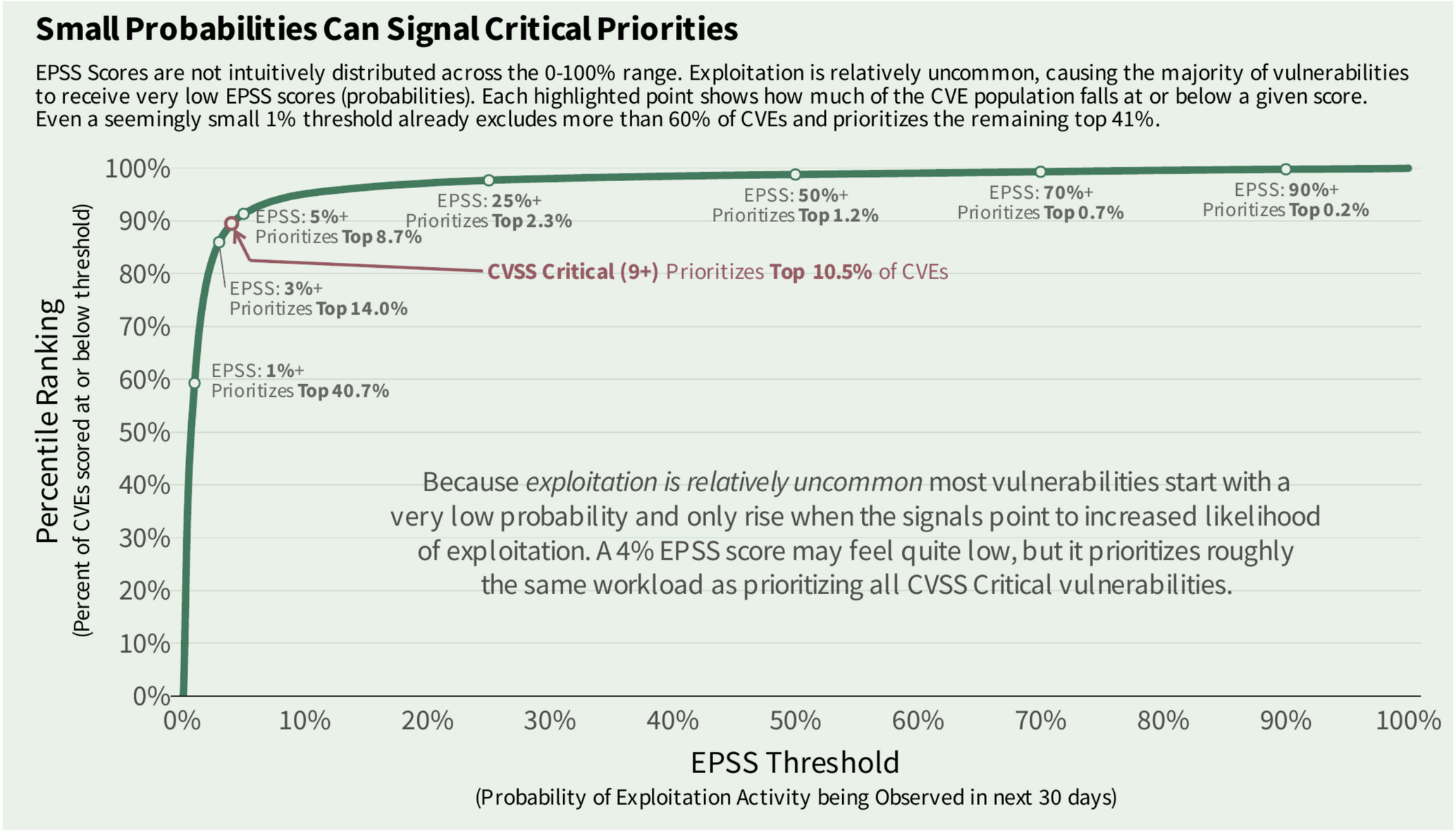
- **Known Ransomware Campaign Use?** **Unknown**
- **CISA BOD 26-04:** **Yes**
- **Date Added:** 2026-10-02
- **Due Date:** 2026-10-05

in accordance with vendor instructions, ensuring compliance with CISA's BOD 26-04 Prioritizing Based on Risk (see URL in Notes) guidance and CISA's "Forensics Triage Requirements" (see URL in Notes). pplicable BOD 26-04 guidance for cloud services or discontinue use of the product if mitigations are unavailable. takeholders are responsible for evaluating each asset's internet exposure and ensuring adherence to BOD 26-04 patching guidelines.

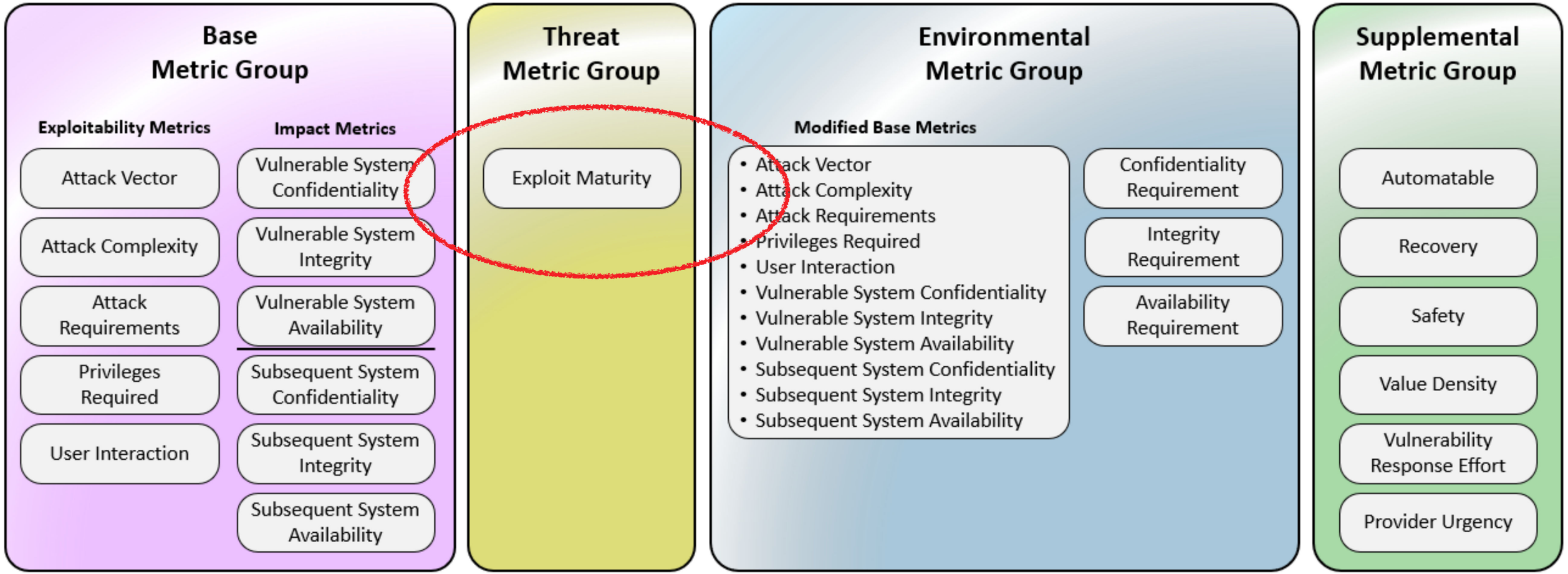
Additional Notes +

NIET LULLEN MAAR PATCHEN
FAMOUS LAST WORDS - DIVD SEPT '26

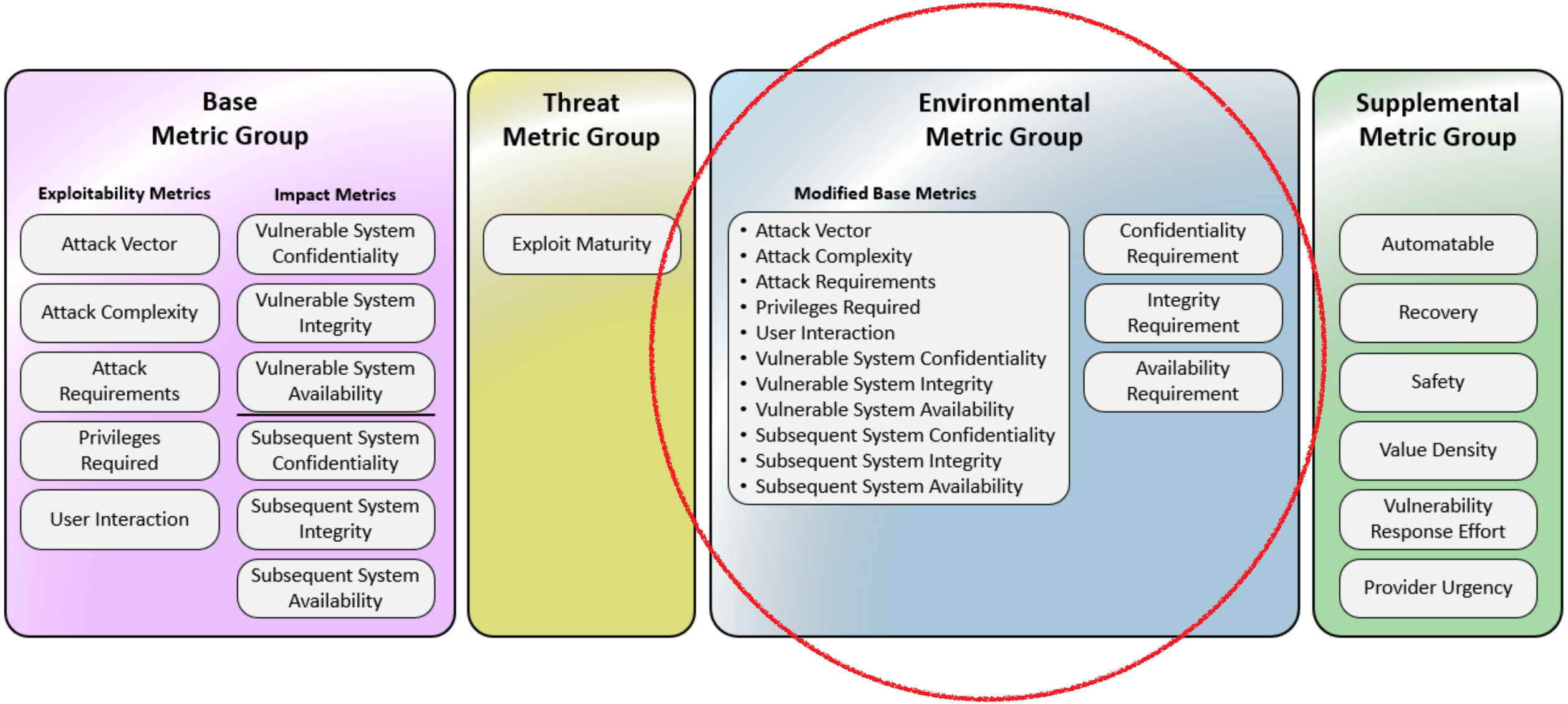
Exploit Prediction Scoring System (EPSS)



CVSS v4.0


Base
Metric Group
Exploitability Metrics
Attack Vector
Attack Complexity
Attack Requirements
Privileges Required
User Interaction
Impact Metrics
Vulnerable System Confidentiality
Vulnerable System Integrity
Vulnerable System Availability
Subsequent System Confidentiality
Subsequent System Integrity
Subsequent System Availability
Threat
Metric Group
Exploit Maturity
Environmental
Metric Group
Modified Base Metrics
• Attack Vector
• Attack Complexity
• Attack Requirements
• Privileges Required
• User Interaction
• Vulnerable System Confidentiality
• Vulnerable System Integrity
• Vulnerable System Availability
• Subsequent System Confidentiality
• Subsequent System Integrity
• Subsequent System Availability
Confidentiality Requirement
Integrity Requirement
Availability Requirement
Supplemental
Metric Group
Automatable
Recovery
Safety
Value Density
Vulnerability Response Effort
Provider Urgency

CVSS v4.0


Base
Metric Group
Exploitability Metrics
Attack Vector
Attack Complexity
Attack Requirements
Privileges Required
User Interaction
Impact Metrics
Vulnerable System Confidentiality
Vulnerable System Integrity
Vulnerable System Availability
Subsequent System Confidentiality
Subsequent System Integrity
Subsequent System Availability
Threat
Metric Group
Exploit Maturity
Environmental
Metric Group
Modified Base Metrics
• Attack Vector
• Attack Complexity
• Attack Requirements
• Privileges Required
• User Interaction
• Vulnerable System Confidentiality
• Vulnerable System Integrity
• Vulnerable System Availability
• Subsequent System Confidentiality
• Subsequent System Integrity
• Subsequent System Availability
Confidentiality Requirement
Integrity Requirement
Availability Requirement
Supplemental
Metric Group
Automatable
Recovery
Safety
Value Density
Vulnerability Response Effort
Provider Urgency

Top 4 Mitigation Strategies - List of Software

) Item(s) | 1 to 10 of 100 | Page 1 of 10

ne	Count	Detection Method
config-6.2.8-30.el7l(n…	41	Active
2-libs-1.0.6-13.el7l(no…	41	Active
klib-2.9.0-11.el7l(none)	41	Active
klib-dicts-2.9.0-11.el7l…	41	Active
tabs-1.11-6.20121102…	41	Active
s-glib-0.100-7.el7l(none)	41	Active
s-python-1.1.1-9.el7l(…	41	Active
check-1.4.1-6.el7l(none)	41	Active
check-lib-1.4.1-6.el7l(…	41	Active
k-4.0.2-4.el7_3.1l(none)	41	Active

Unsupported Product Summary - Operating Systems

Fedora	Ubuntu	Slackware
Debian	Mandrake	Mac OS X
CentOS	openSUSE	Microsoft

Last Updated: 16 minutes ago

CSF - Browser Summary

Chrome	9	Microsoft Edge	0
Firefox	2	Safari	0
Internet Explorer	23	Opera	0

Last Updated: 1 minute ago

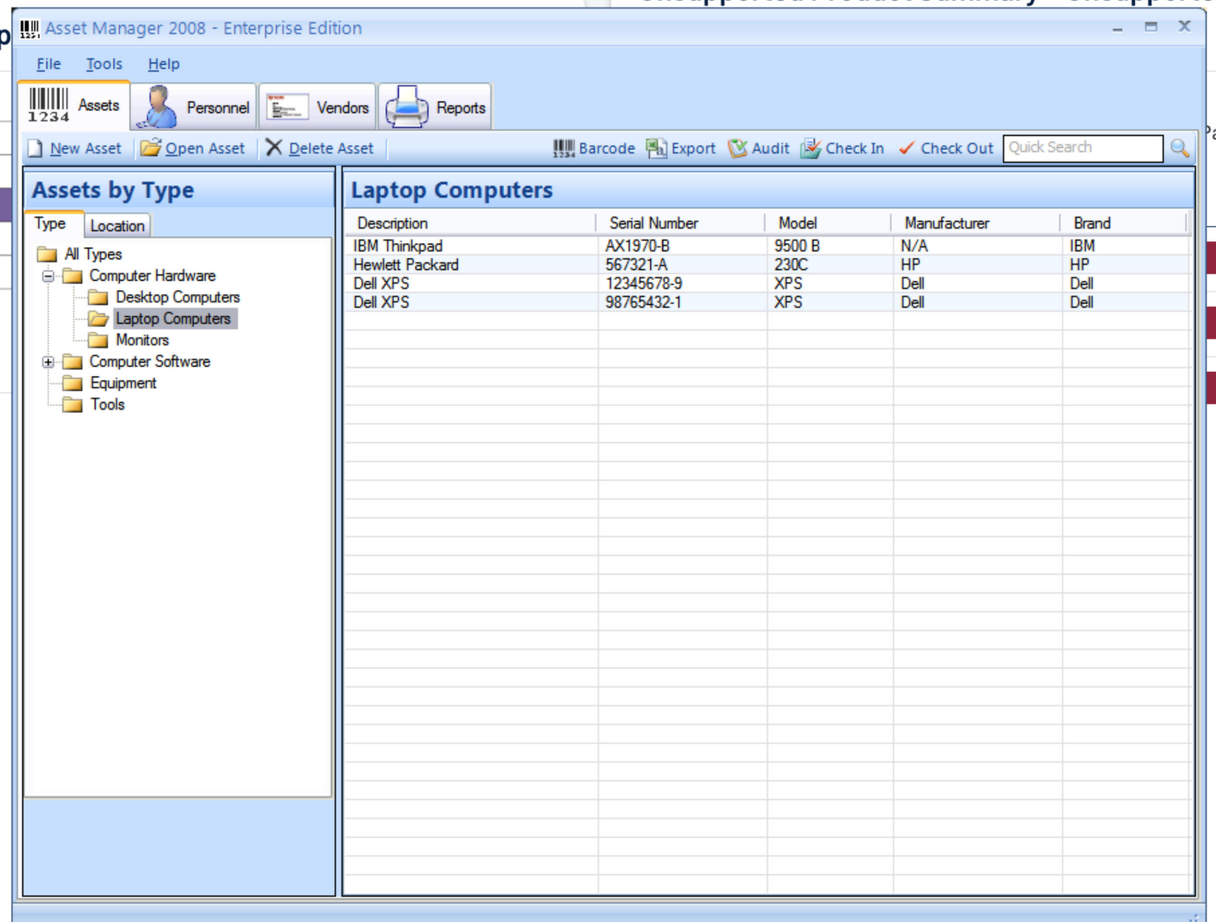
CSF - Software Ap

Adobe Acrobat
Adobe Photoshop
MS Office
MS Office 365
MS Office for Mac

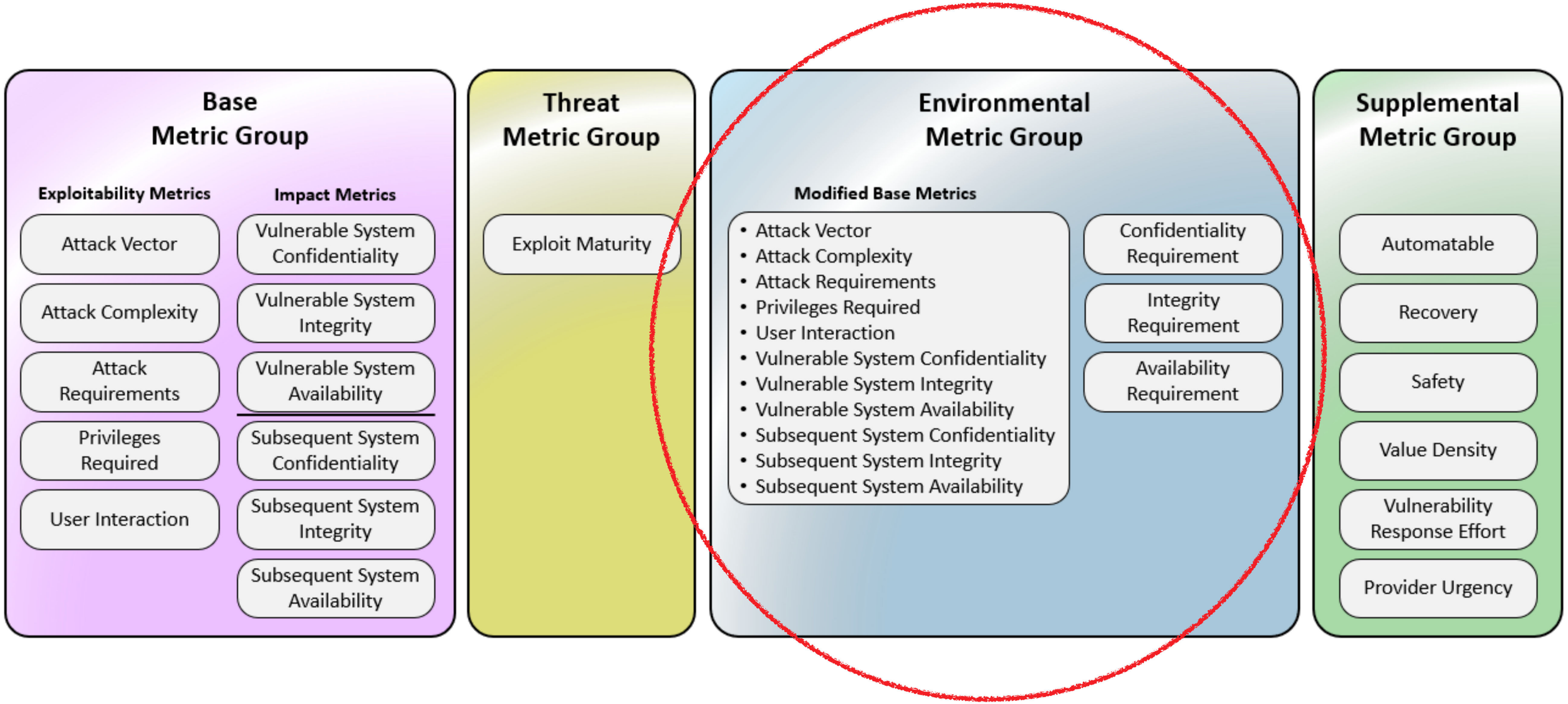
Unsupported Product Summary - Unsupported

Page 1 of 6

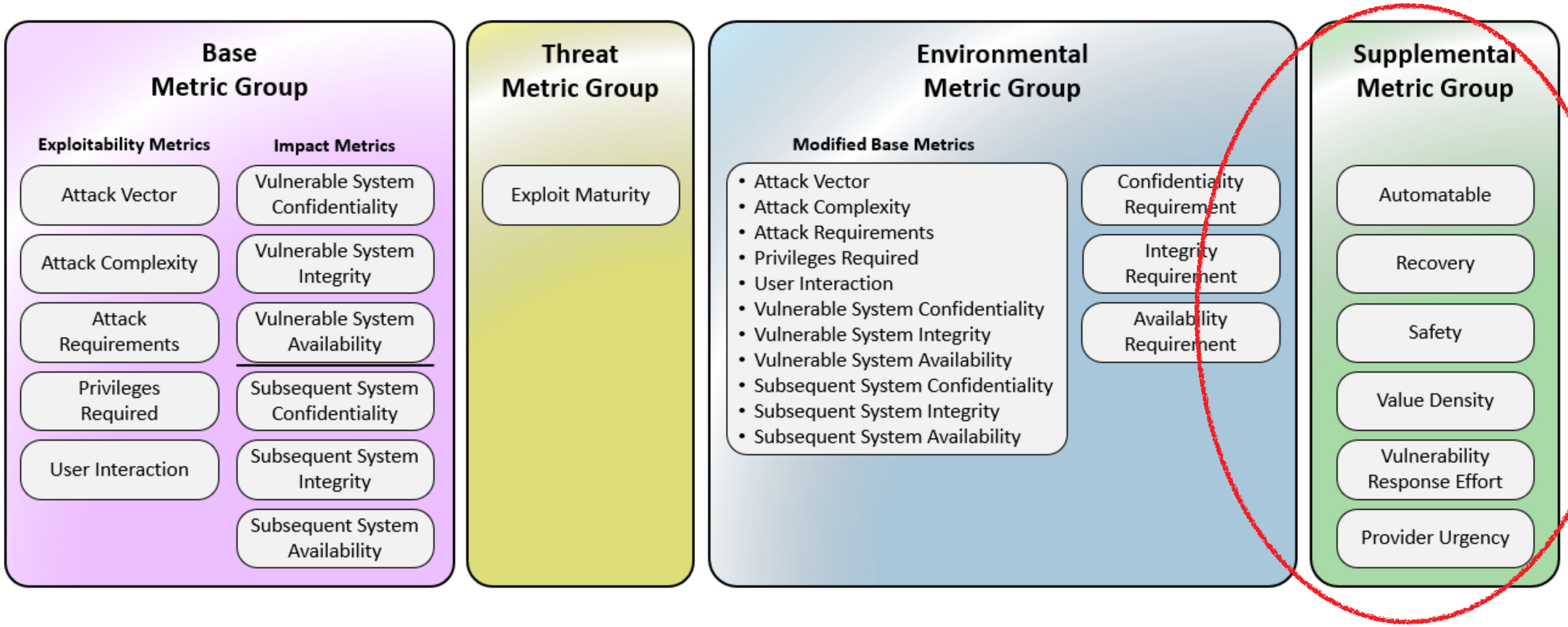
Total
229
24
11



CVSS v4.0

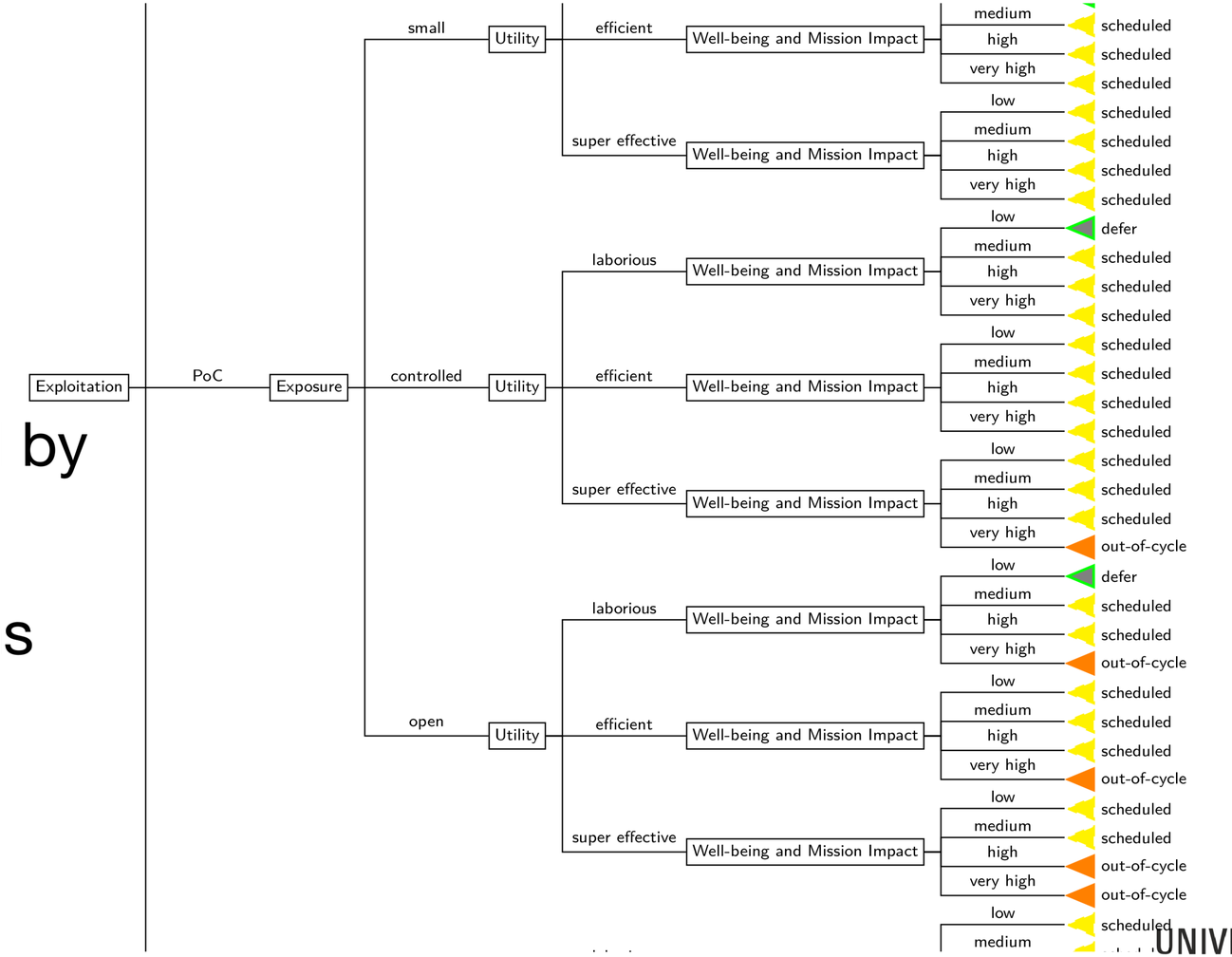

Base
Metric Group
Exploitability Metrics
Attack Vector
Attack Complexity
Attack Requirements
Privileges Required
User Interaction
Impact Metrics
Vulnerable System Confidentiality
Vulnerable System Integrity
Vulnerable System Availability
Subsequent System Confidentiality
Subsequent System Integrity
Subsequent System Availability
Threat
Metric Group
Exploit Maturity
Environmental
Metric Group
Modified Base Metrics
• Attack Vector
• Attack Complexity
• Attack Requirements
• Privileges Required
• User Interaction
• Vulnerable System Confidentiality
• Vulnerable System Integrity
• Vulnerable System Availability
• Subsequent System Confidentiality
• Subsequent System Integrity
• Subsequent System Availability
Confidentiality Requirement
Integrity Requirement
Availability Requirement
Supplemental
Metric Group
Automatable
Recovery
Safety
Value Density
Vulnerability Response Effort
Provider Urgency

CVSS v4.0

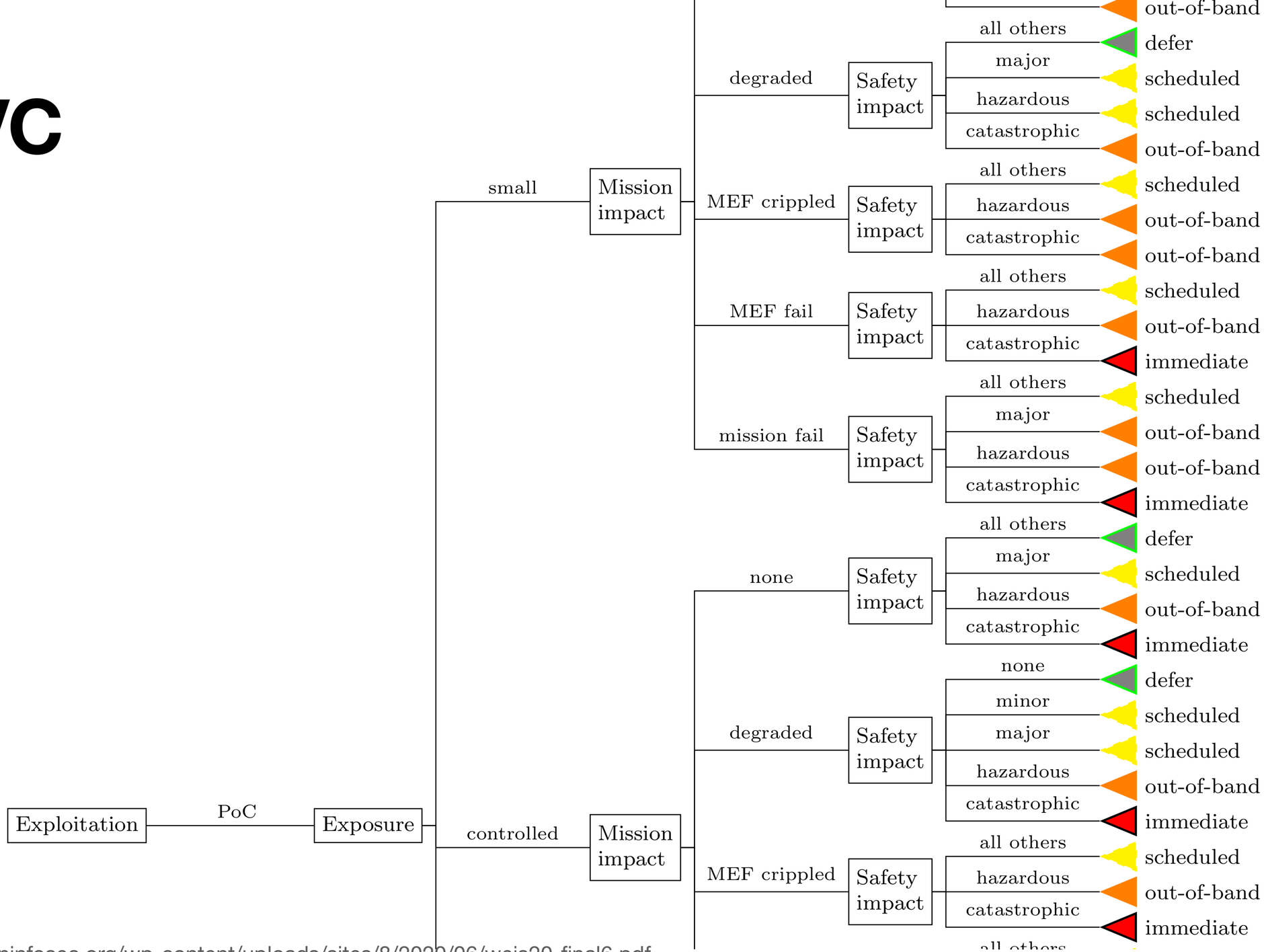

Base
Metric Group
Exploitability Metrics
Attack Vector
Attack Complexity
Attack Requirements
Privileges Required
User Interaction
Impact Metrics
Vulnerable System Confidentiality
Vulnerable System Integrity
Vulnerable System Availability
Subsequent System Confidentiality
Subsequent System Integrity
Subsequent System Availability
Threat
Metric Group
Exploit Maturity
Environmental
Metric Group
Modified Base Metrics
• Attack Vector
• Attack Complexity
• Attack Requirements
• Privileges Required
• User Interaction
• Vulnerable System Confidentiality
• Vulnerable System Integrity
• Vulnerable System Availability
• Subsequent System Confidentiality
• Subsequent System Integrity
• Subsequent System Availability
Confidentiality Requirement
Integrity Requirement
Availability Requirement
Supplemental
Metric Group
Automatable
Recovery
Safety
Value Density
Vulnerability Response Effort
Provider Urgency

SSVC - Decision Trees

- Simple decision trees
- Result is an action
- Outcome on the right is defined by risk-appetite
  - Easily tunable to organisations
- Provides a simple audit trail for decisions



SSVC



https://weis2020.econinfosec.org/wp-content/uploads/sites/8/2020/06/weis20-final6.pdf

Possible Decision Points in the Tree

Technical properties
Same for everyone

- Exploitation (None, PoC, Active)
- Technical Impact (partial, total)
- Utility for Attacker
  (laborious, efficient, supereffective)
  - Automatable
  - Value Density

Contextual properties
Different for everyone

- WellBeing and Mission Impact
  (low, medium, high, very-high)
  - Safety Impact
  - Mission Impact
- System Exposure (small, controlled, open)

https://github.com/CERTCC/SSVC

Possible Decision Points in the Tree

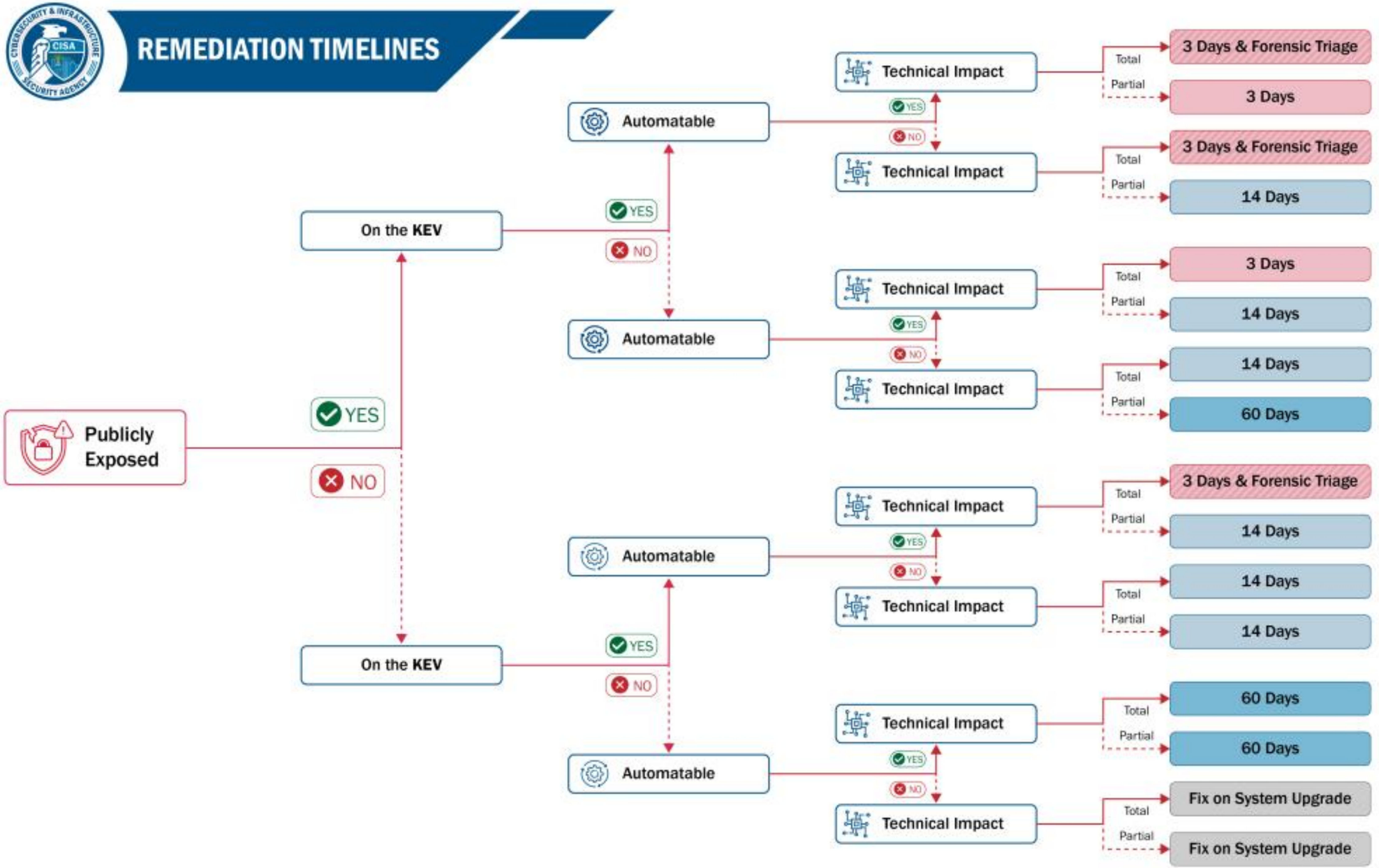
Technical properties
Same for everyone

- Exploitation (None, PoC, Active)
- Technical Impact (partial, total)
- Utility for Attacker
  (laborious, efficient, supereffective)
- Automatable
- Value Density

Contextual properties
Different for everyone

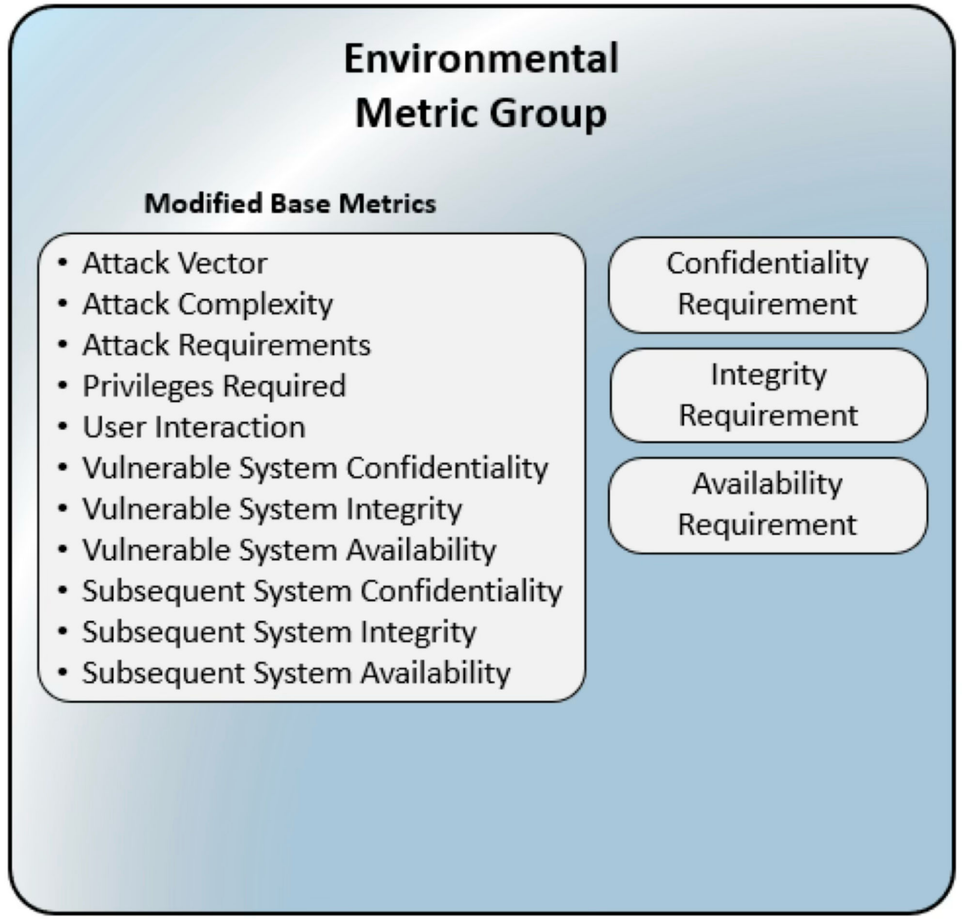
- WellBeing and Mission Impact
  (low, medium, high, very-high)
- Safety Impact
- Mission Impact
- System Exposure (small, controlled, open)

https://github.com/CERTCC/SSVC



https://www.cisa.gov/news-events/directives/bod-26-04-prioritizing-security-updates-based-risk

Vulnerability Decision Points



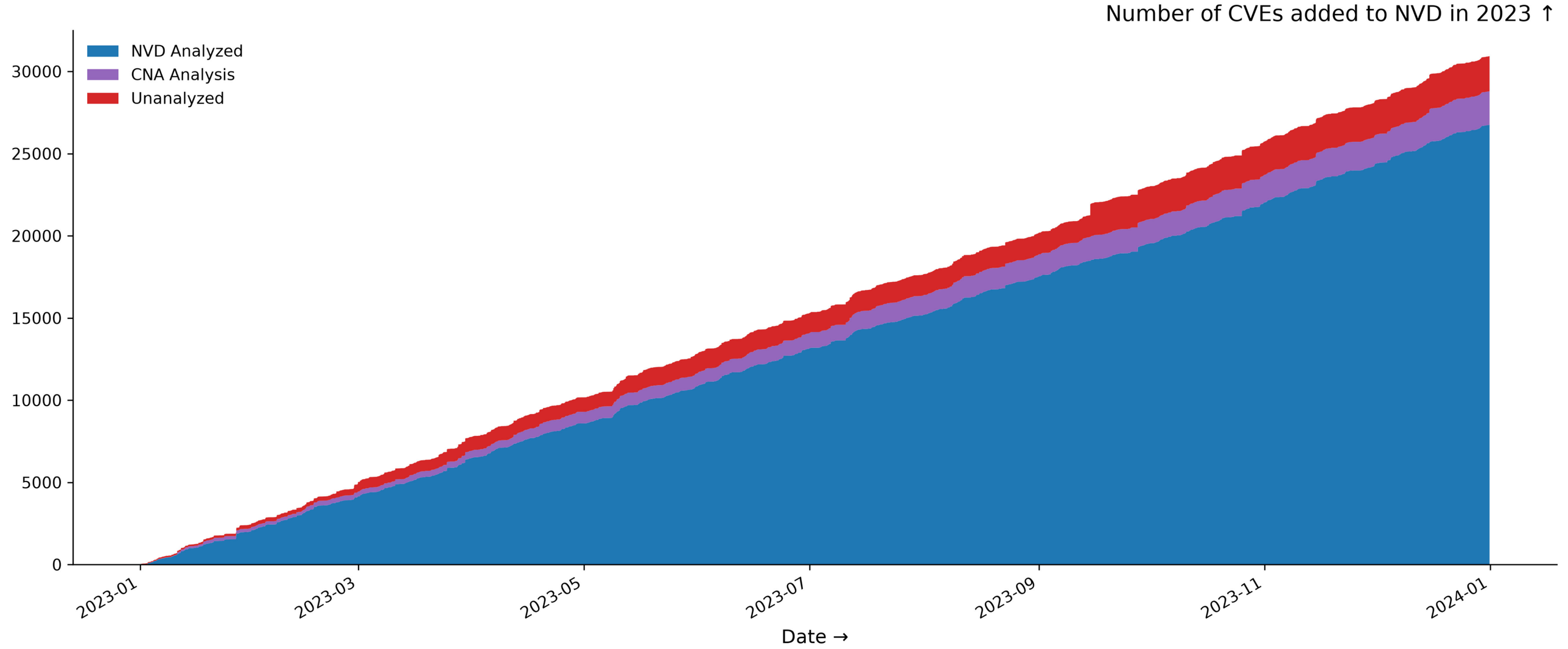
Business Perspective

- WellBeing and Mission Impact
  (low, medium, high, very-high)
  - Safety Impact
  - Mission Impact
- System Exposure (small, controlled, open)

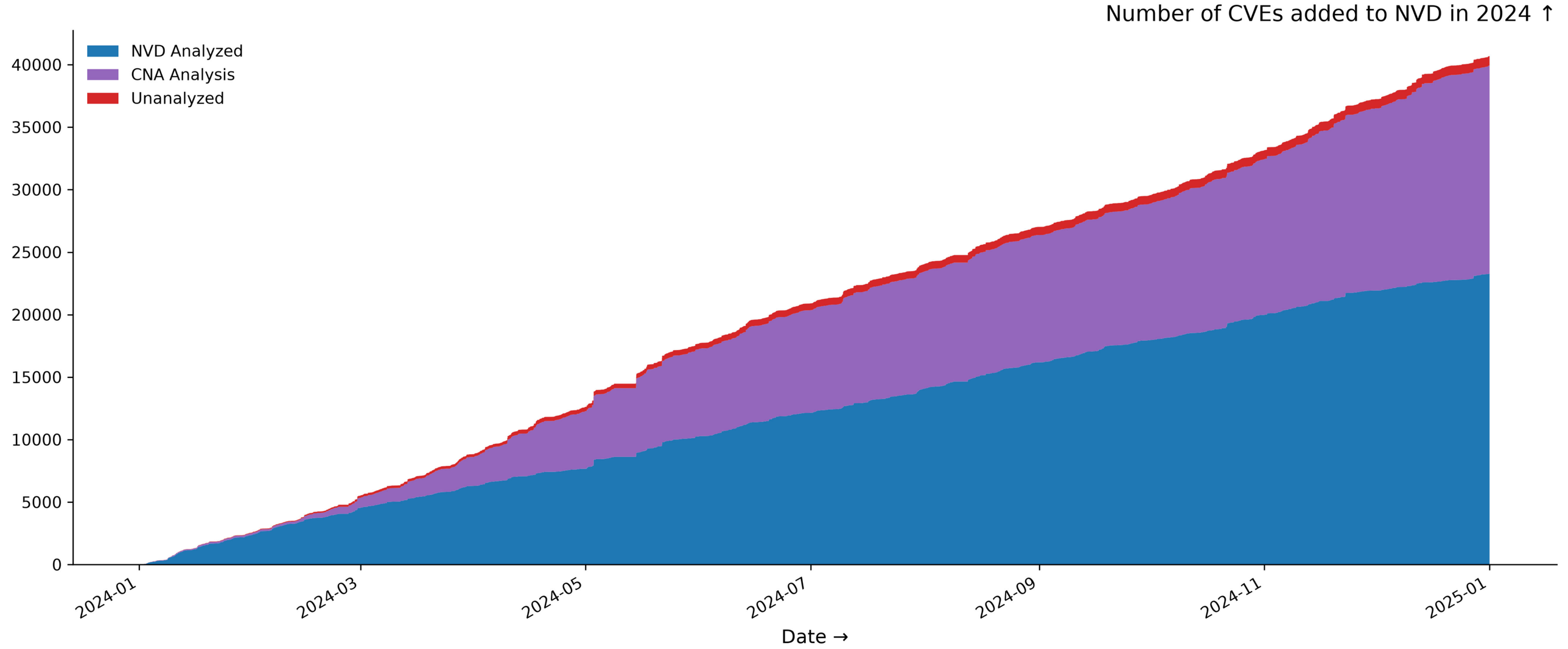
https://github.com/CERTCC/SSVC

Final thoughts

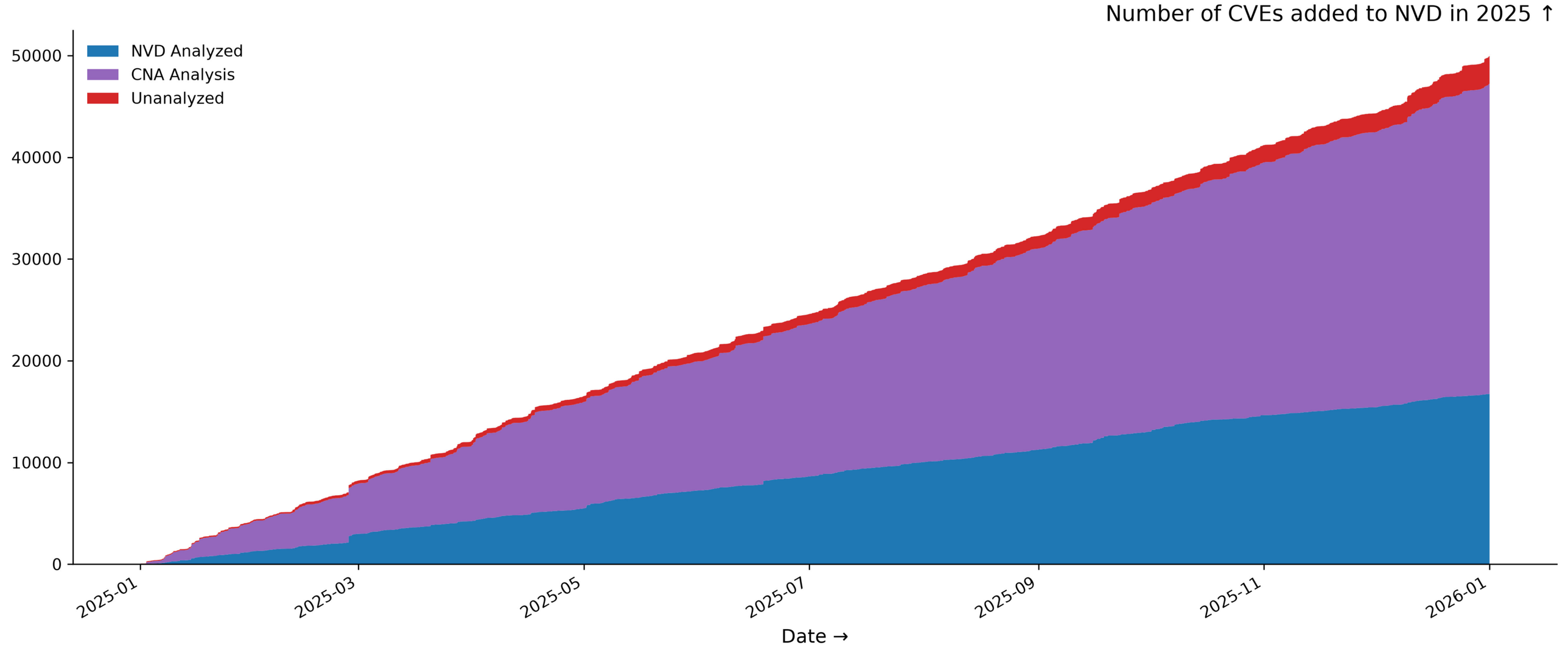
- More data is not more better
- Especially when the source of that data has changed



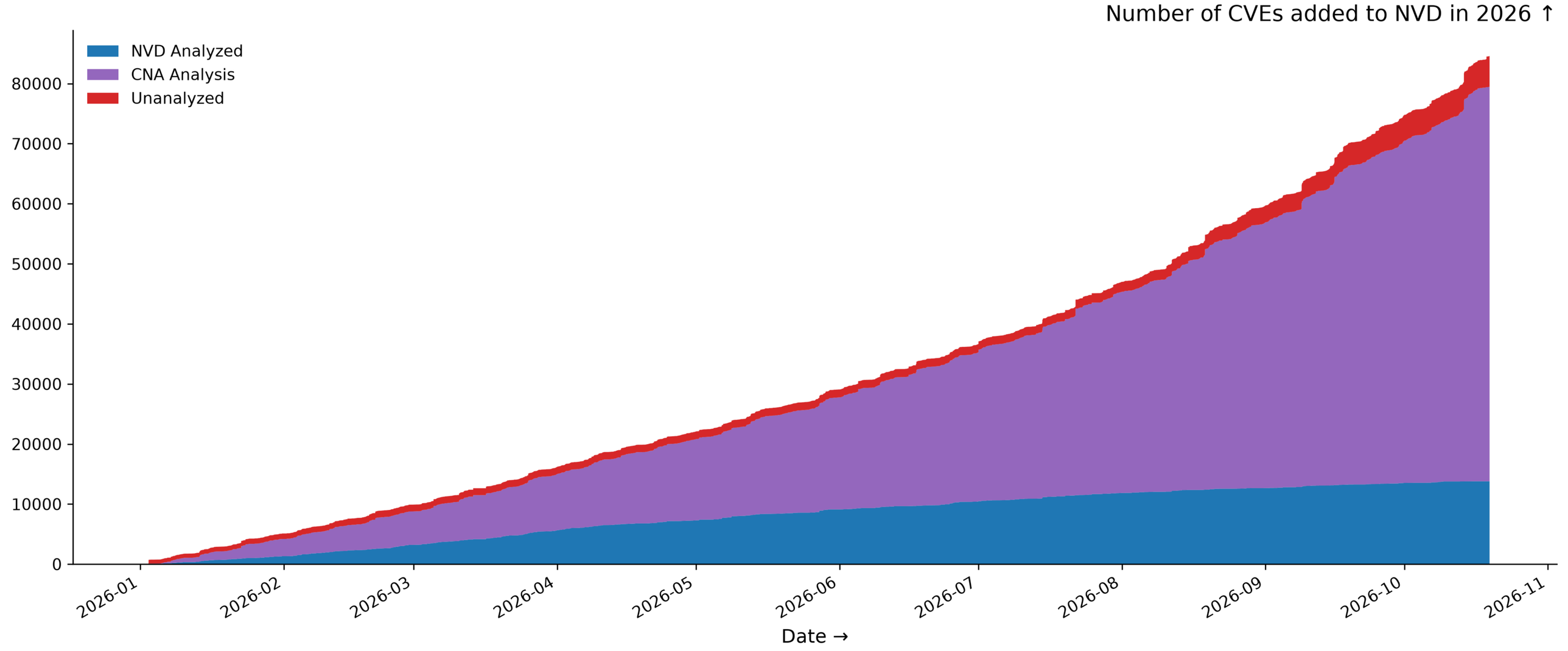
UNIVERSITY
OF TWENTE.



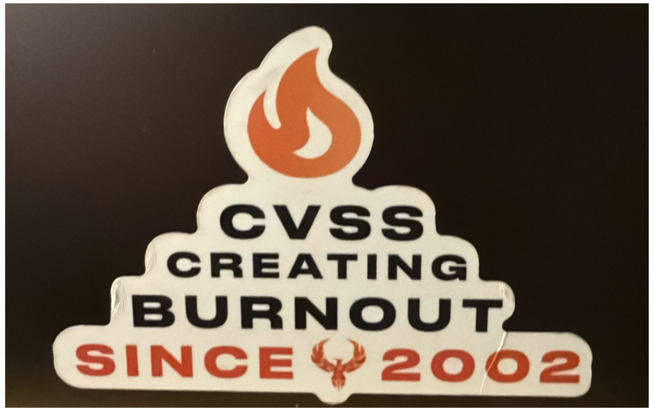
UNIVERSITY
OF TWENTE.



UNIVERSITY OF TWENTE.



UNIVERSITY OF TWENTE.

Final thoughts

- More data is not more better
- Especially when the source of that data has changed (!)
- Vulnerability Management must explicitly include business context
- Doing that will actually make it more efficient!