Gestão de Vulnerabilidades: Entendendo CVSS, EPSS, SSVC, CVD e VDP

Cristine Hoepers, D.Sc.
Gerente, CERT.br/NIC.br
cristine@cert.br

12º Fórum Brasileiro de CSIRTs
São Paulo, SP – 29 de julho de 2024

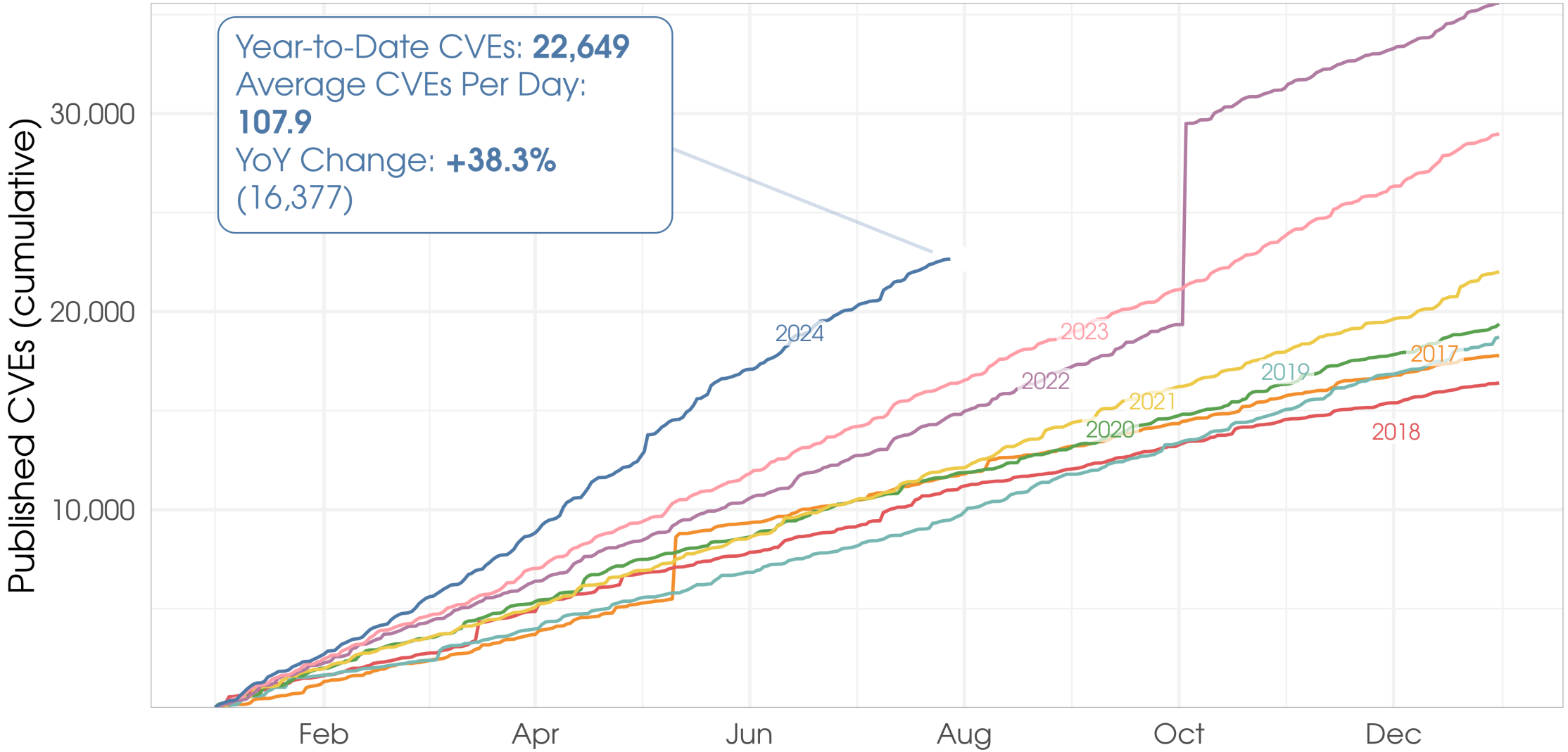
cert.br nic.br cgi.br


EPSS
CVSS
CWE
NVD
SBOM
SSVC
VDP
VEX
CVD
CSAF
KEV
CVE
CNA

TLP:CLEAR

Year-to-date CVE publications (MITRE CVE List)

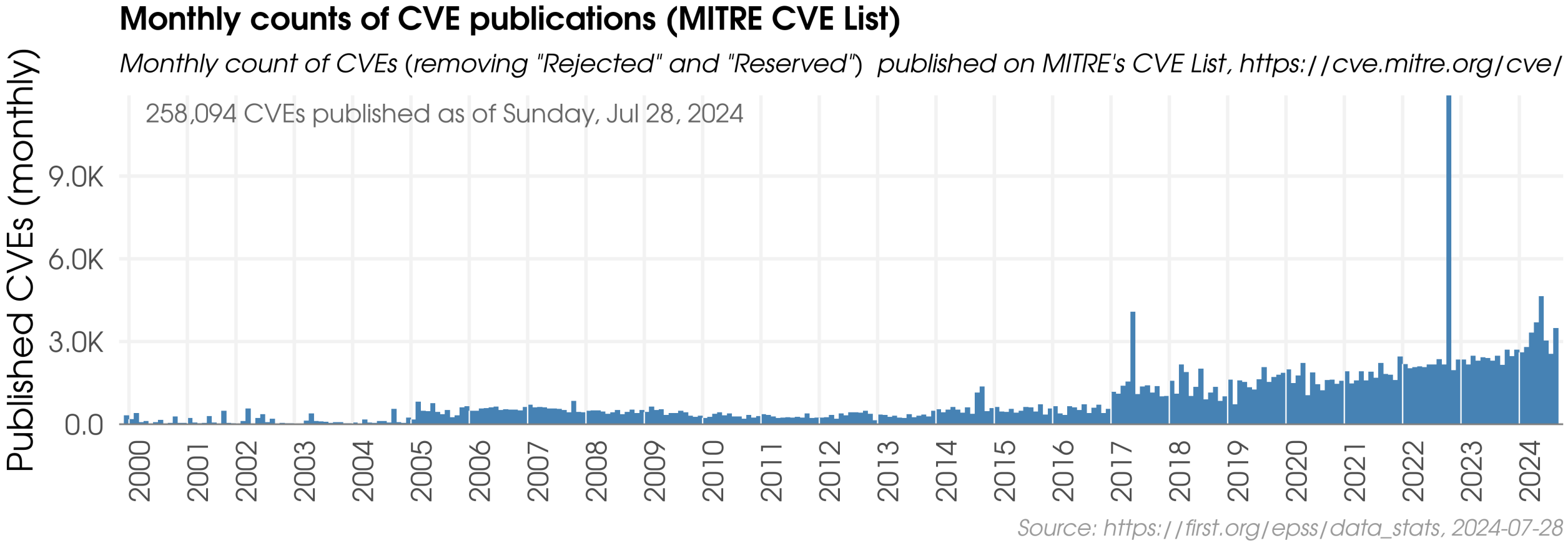
Lines showing the daily cumulative count of published CVEs on MITRE's CVE List, https://cve.mitre.org/cve/



Fonte: https://www.first.org/epss/data_stats

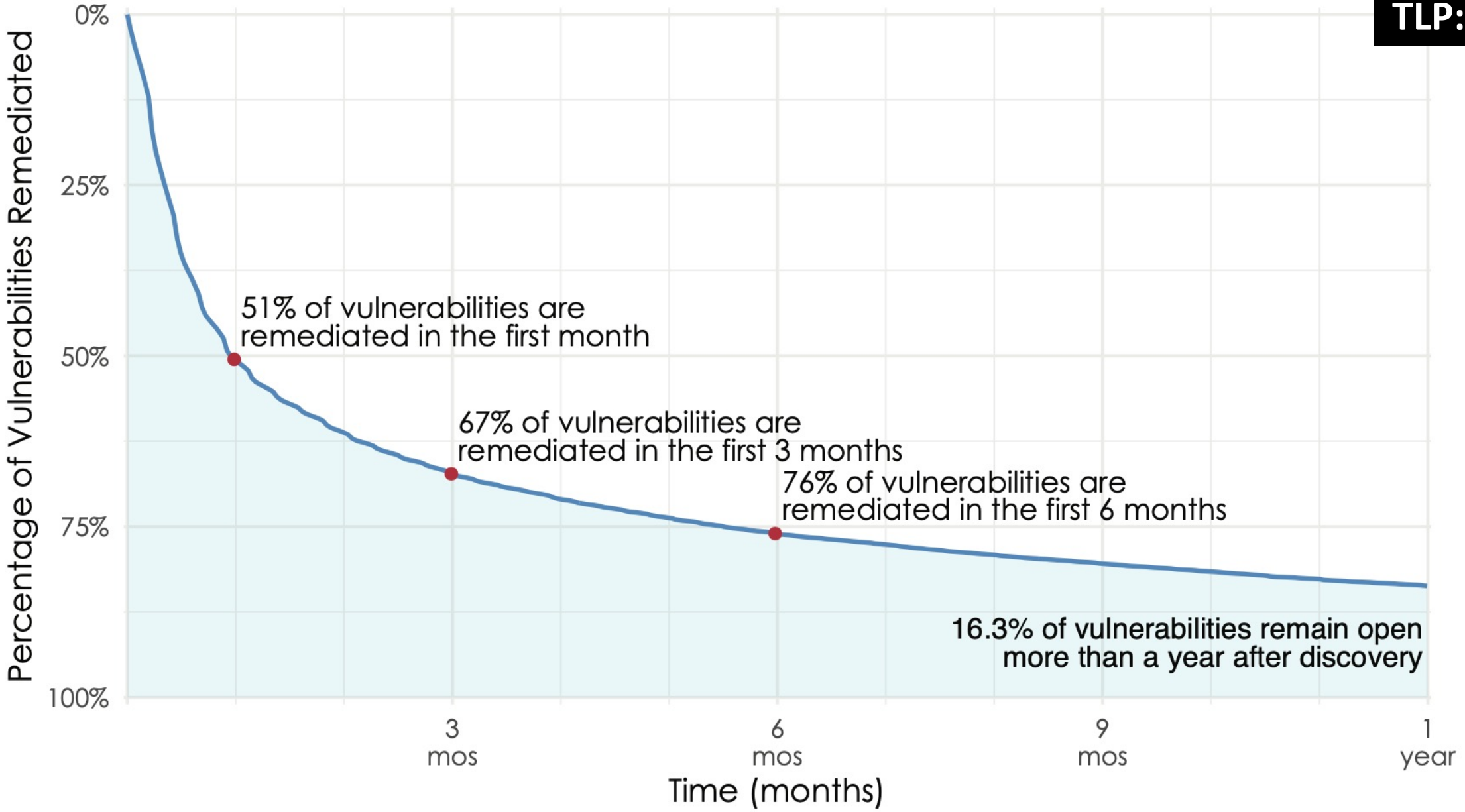
Source: https://first.org/epss/data_stats, 2024-07-28

TLP:CLEAR



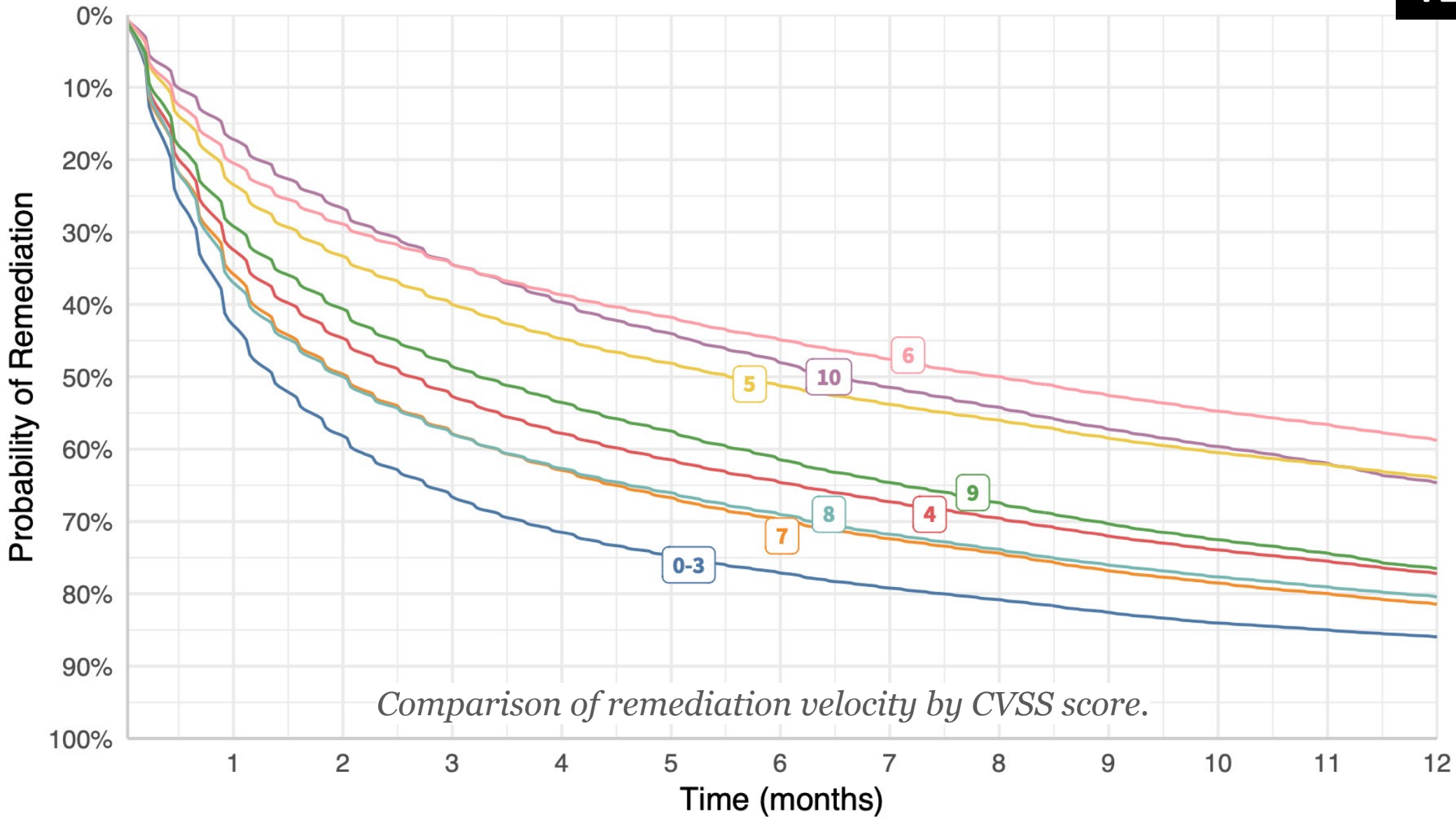
Fonte: https://www.first.org/epss/data_stats

TLP:CLEAR



Fonte: https://www.cyentia.com/patching-fast-and-slow/ | https://www.cyentia.com/why-your-mttr-is-probably-bogus/

TLP:CLEAR



Comparison of remediation velocity by CVSS score.

Fonte: https://www.cyentia.com/patching-fast-and-slow/

Gestão de Vulerabilidades

“A prática de identificar, priorizar e corrigir vulnerabilidades de *software* conhecidas.”

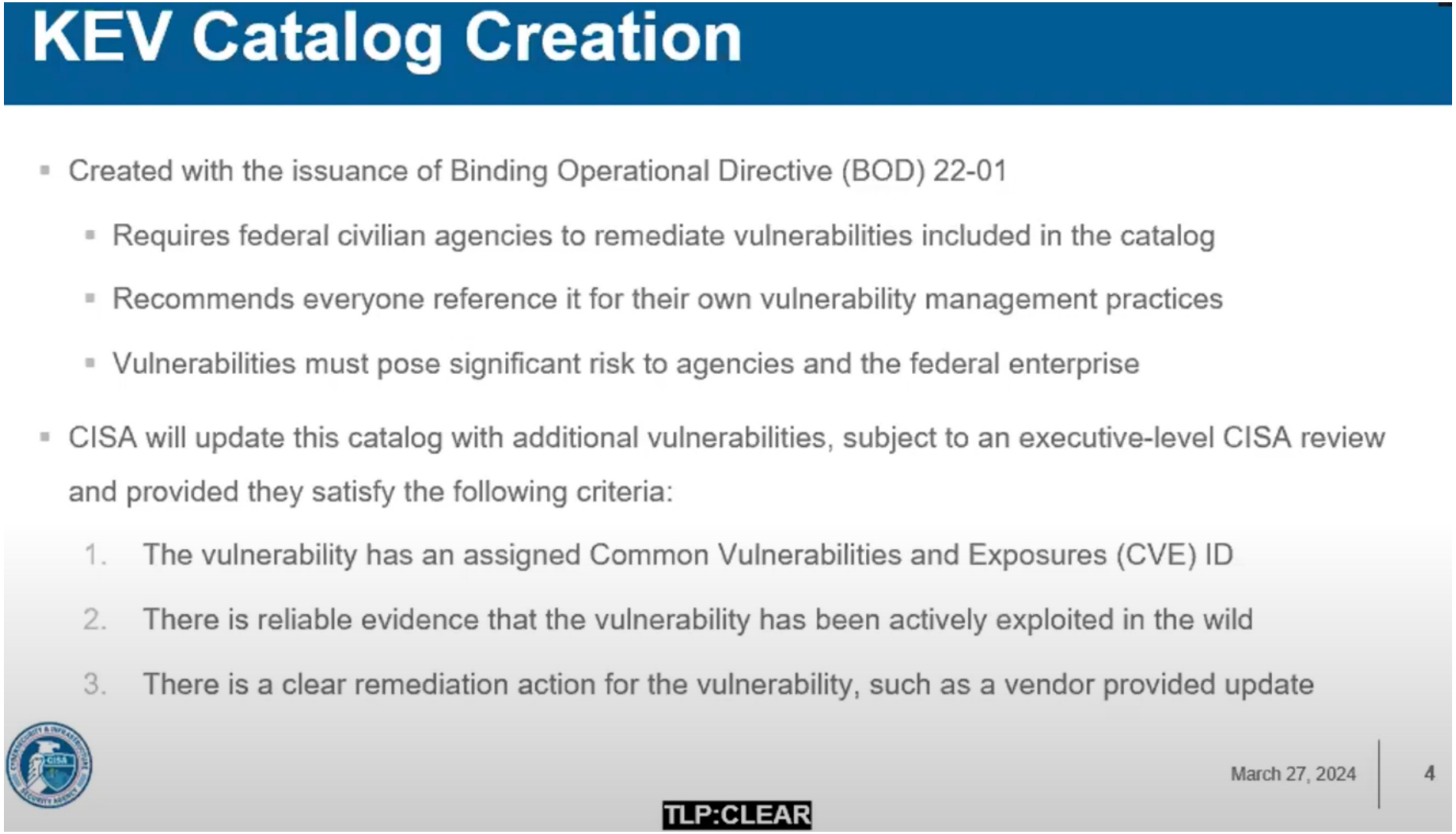
Alguns fatos:

- Mais da metade das organizações só conseguem aplicar patches em 15.5% dos CVEs/mês
  - ¼ corrige menos de 6.6% dos CVEs
- Menos de 5% dos CVEs são ativamente explorados
- CVSS **não** é uma métrica de priorização
- 32% das top 100 vulnerabilidades exploradas na lista do ShadowServer são “*vintage vulnerabilities*”
- CISA KEV (*Known Exploited Vulnerabilities*) tem 46% de “*vintage vulnerabilities*”

Fontes:
https://arxiv.org/pdf/2302.14172
https://www.first.org/resources/papers/vulncon2024/VulnCon-Why-Can-t-We-All-Just-Get-Along.pdf

Antes de Avançarmos: O que é o CISA KEV

TLP:CLEAR

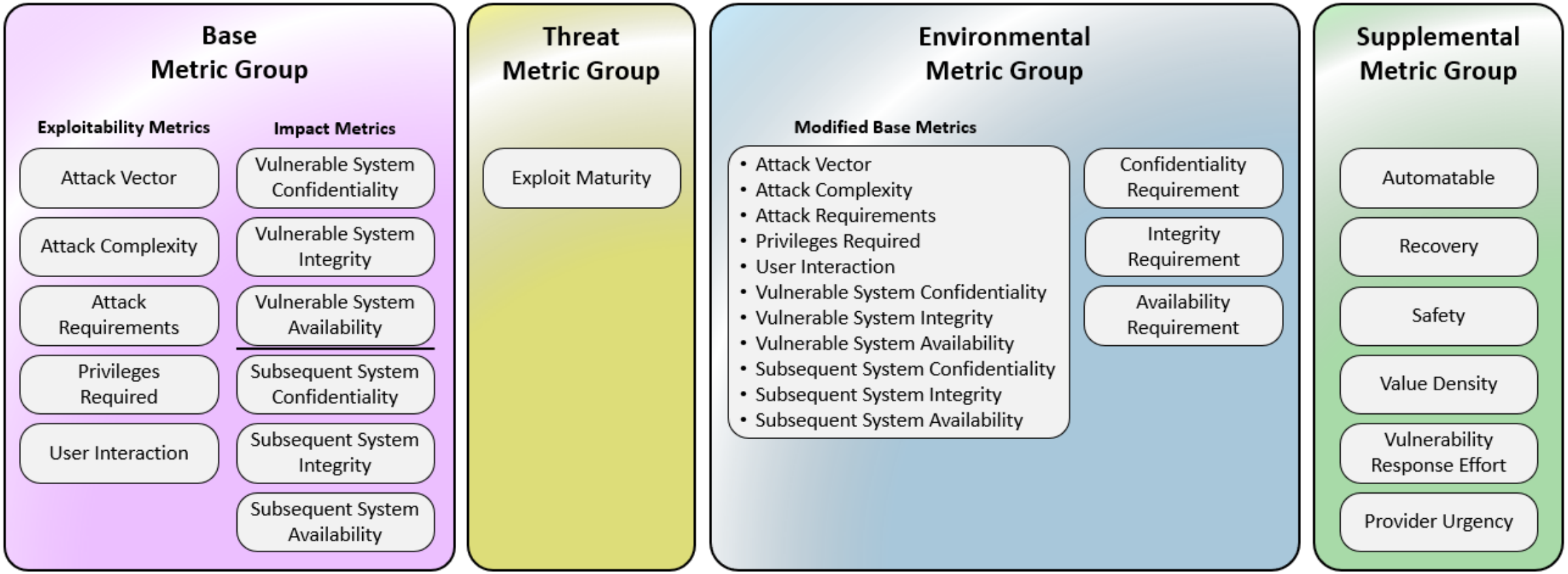


Fonte: CISA's Known Exploited Vulnerabilities (KEV) Catalog, CVE/FIRST VulnCon 2024 & Annual CNA Summit
https://youtu.be/T4kYHm54SM0?feature=shared&t=210

Antes de Avançarmos: CVSS v4.0

TLP:CLEAR

"The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities."



Fonte: Common Vulnerability Scoring System version 4.0: Specification Document
https://www.first.org/cvss/v4.0/specification-document

Risco = Vulnerabilidade + Ameaça + Impacto

Gestão de Vulnerabilidades com Base em Risco

Nesse contexto a pergunta é:

> Qual o risco de uma vulnerabilidade ser ativamente explorada **e** causar um impacto negativo?

Ou seja, **quais patches** eu preciso **aplicar agora e quais podem esperar** a próxima janela de manutenção?

Abordagens:

– Específicas de sistemas operacionais (como Microsoft e RedHat)

– Proprietárias (como Tenable, Rapid7 e RecordedFuture)

– Padrões abertos (como EPSS e SSVC)

Fonte: https://arxiv.org/pdf/2302.14172

Alguns Padrões para Informar as Decisões de Risco: CVSS, EPSS e SSVC

TLP:CLEAR

CVSS – Common Vulnerability Scoring System

– Uma pontuação relativa à **severidade** de uma vulnerabilidade
  – ex: execução remota de código sem interação vs. necessidade de conta no sistema para posterior escalação de privilégio

EPSS – Exploit Prediction Scoring System

– **Probabilidade de** uma vulnerabilidade **ser ativamente explorada** nos próximos 30 dias

SSVC – Stakeholder-Specific Vulnerability Categorization

– Uma **metodologia para priorizar** vulnerabilidades com base nas necessidades das partes interessadas
  – Criada pelo CERT Division SEI/CMU em conjunto com a CISA
  – CISA instituiu um processo específico para o Governo dos EUA

https://www.first.org/epss/

“The Exploit Prediction Scoring System (EPSS) is a data-driven effort for estimating the likelihood (probability) that a software vulnerability will be exploited in the wild.”

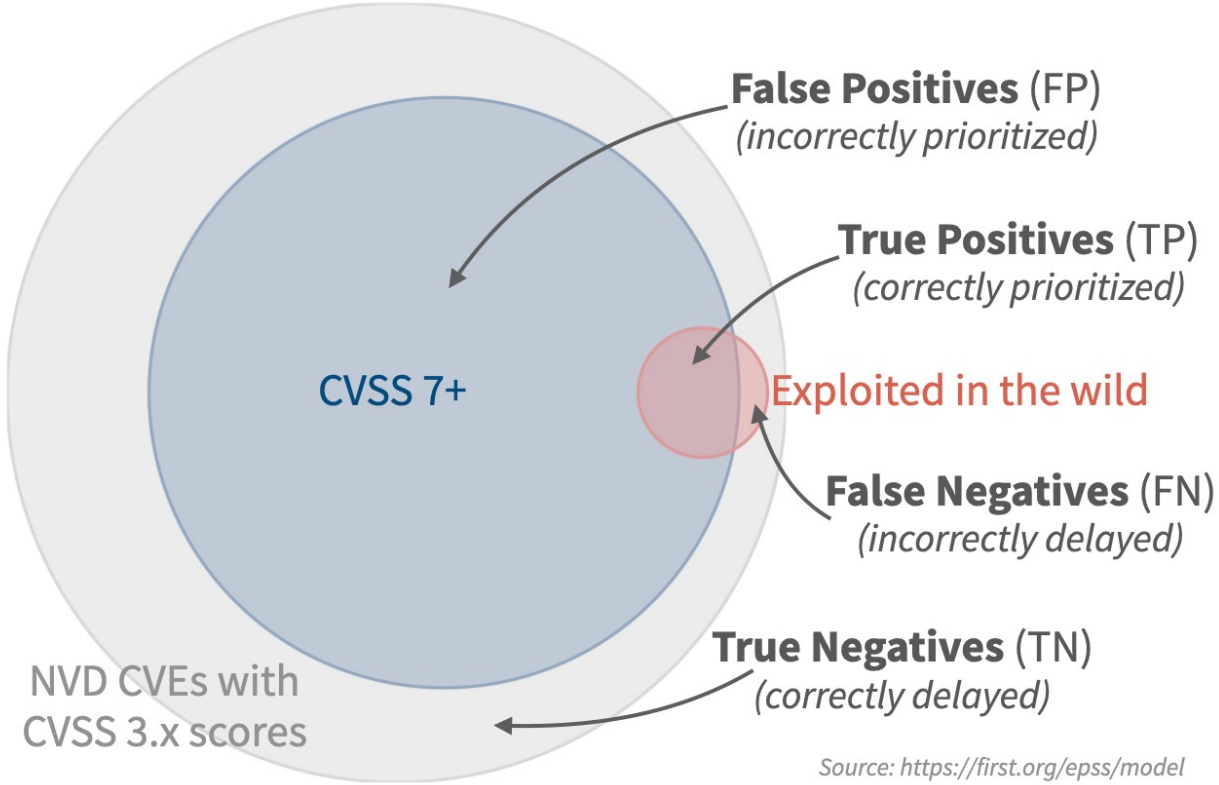
- Objetivo: ajudar as organizações a terem a melhor cobertura de aplicação de patches com o menor esforço (já que recursos são limitados)
- Dados levados em conta para o cálculo da pontuação: Idade do CVE, CPE, CWE, CVSS 3.x, CISA KEV, Google Project Zero, Trend Micro's Zero Day Initiative (ZDI), Exploit-DB, GitHub, MetaSploit, Intrigue, sn1per, jaeles, nuclei, entre outros
- Quem usa:
  - https://www.first.org/epss/who_is_using/
- Ferramentas Open Source:
  - https://www.first.org/epss/epss_tools
- Dados completos – arquivo CSV atualizado diariamente:
  - https://www.first.org/epss/data_stats

Efetividade do EPSS na Vida Real

Metodologia

- 1 ano de dados usados para treinar o modelo
  - CVEs publicados entre 01/11/2021 – 31/10/2022
- Período de teste: dezembro/2022
- Avaliar para este mês
  - predições do EPSS versus
  - outras estratégias de priorização

Entendendo os Gráficos do próximo *slide*



Fonte: https://arxiv.org/pdf/2302.14172

TLP:CLEAR

Exploit:Exploit DB

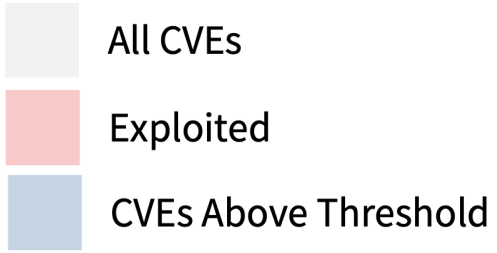
Effort: **10.9% of CVEs**
Coverage: **34.7%**
Efficiency: **13.0%**

Exploit:metasploit

Effort: **1.0% of CVEs**
Coverage: **14.9%**
Efficiency: **60.5%**

Site:KEV

Effort: **0.5% of CVEs**
Coverage: **5.9%**
Efficiency: **53.2%**



CVSS v3.x

Threshold: **7+**
Effort: **58.1% of CVEs**
Coverage: **82.1%**
Efficiency: **3.9%**

CVSS v3.x

Threshold: **9.1+**
Effort: **15.1% of CVEs**
Coverage: **33.5%**
Efficiency: **6.1%**

EPSS v3

Threshold: **0.088+**
Effort: **7.3% of CVEs**
Coverage: **82.0%**
Efficiency: **45.5%**

EPSS v3

Threshold: **0.022+**
Effort: **15.3% of CVEs**
Coverage: **90.4%**
Efficiency: **24.1%**

Fonte: https://arxiv.org/pdf/2302.14172

SSVC - Stakeholder-Specific Vulnerability Categorization

- Uma árvore de decisão, que determina como priorizar e tratar uma vulnerabilidade
- A árvore leva em conta as seguintes propriedades:
  - Evidência de uma vulnerabilidade estar sendo ativamente explorada
  - Impacto técnico
  - Impacto em *safety*
  - Exposição do ativo
- Relação com CVSS e EPSS
  - CVSS pode ser usado para informar a decisão de impacto técnico
  - EPSS pode ser usado para decidir a probabilidade e/ou evidência de estar sendo ativamente explorado

Priority	Description
Defer	Do not act at present
Scheduled	Act during regularly scheduled maintenance.
Out-of-Band	Act more quickly than usually
Immediate	Act immediately

Fontes: Learning SSVC – https://certcc.github.io/SSVC/tutorials/

Stakeholder-Specific Vulnerability Categorization (SSVC), Technical Report
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=636379

Risco = Vulnerabilidade + Ameaça + Impacto

+

+ SSVC

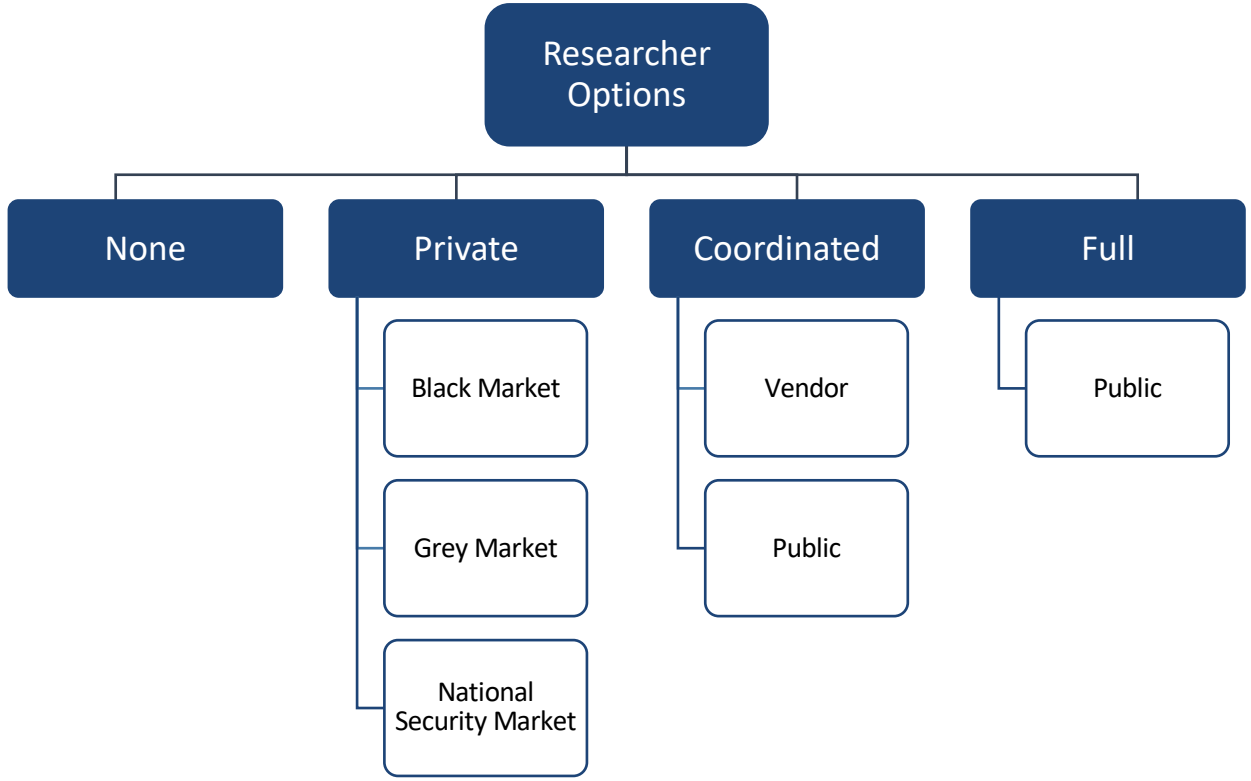
CVD, VDP & Bug Bounties

cert.br nic.br cgi.br

Divulgação de Informações Sobre Vulnerabilidades

Opções de divulgação de quem descobre uma vulnerabilidade:

- Esconder a existência.
- Vender para uma entidade privada.
- Tentar contatar o fabricante ou uma organização para realizar a divulgação de forma coordenada, somente após haver uma correção.
- Divulgar imediatamente de forma pública.



Boas Práticas para Comunicação com o Vendor:
CVD – Coordinated Vulnerability Disclosure

TLP:CLEAR

Fases:

- Descoberta
- Notificação
- Validação e triagem
- Remediação
- Divulgação
- Implantação

Um processo para:

- Dar chances de defesa antes da exploração de uma vulnerabilidade
- Reduzir as vantagens dos adversários

Princípios:

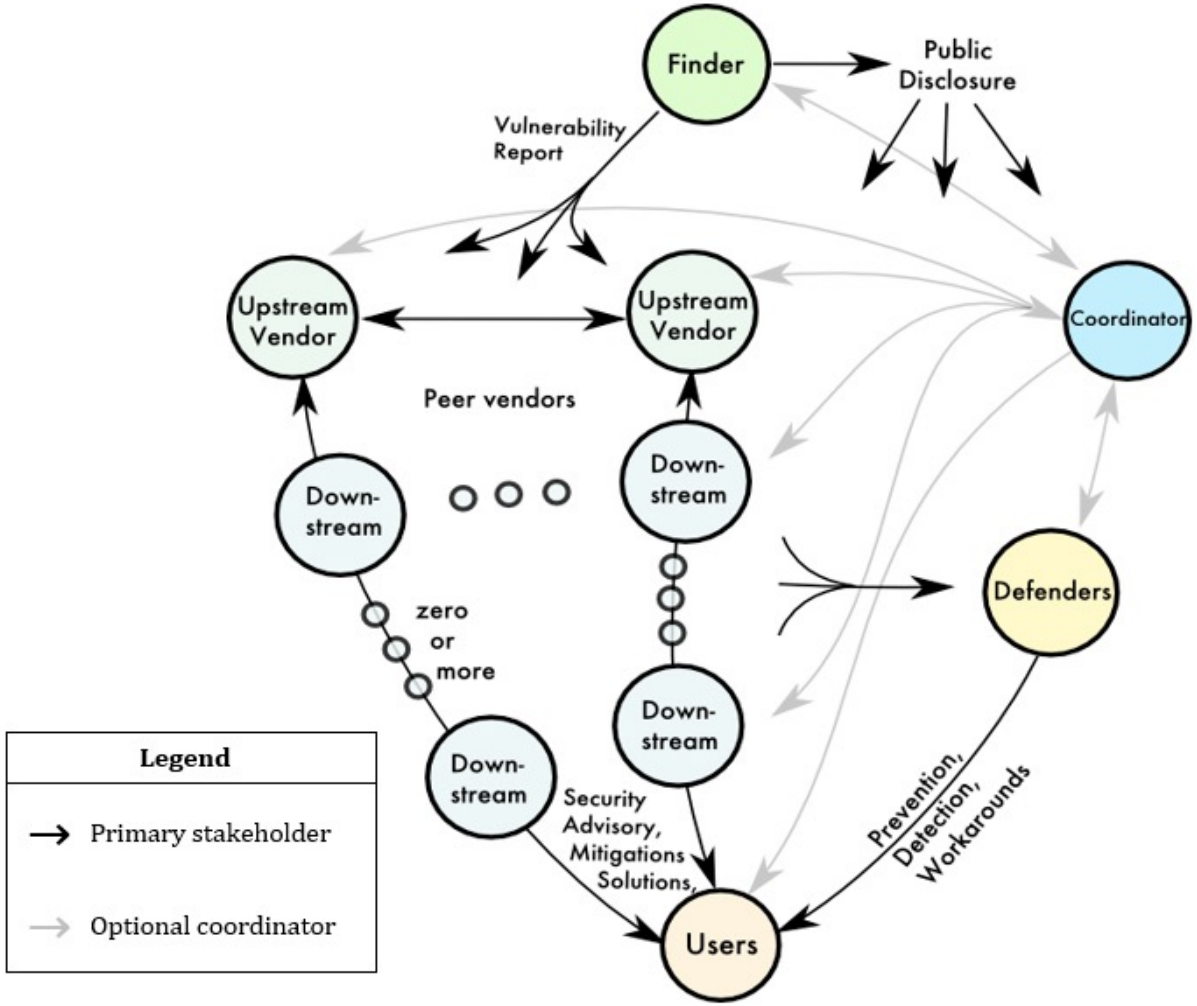
- Reduzir danos
- Presumir benevolência
- Evitar surpresas
- Incentivar o comportamento desejado
- Considerar práticas éticas
- Melhorar processos

Fontes:
https://certcc.github.io/CERT-Guide-to-CVD/
https://www.enisa.europa.eu/topics/vulnerability-disclosure
https://www.cisa.gov/coordinated-vulnerability-disclosure-process

TLP:CLEAR

A Vida Real é Mais Complexa:
Multi-Party Vulnerability Coordination and Disclosure

- As normas ISO focam em coordenação com um único ator: o *vendor*
- Vida real é mais complexa:
  - bibliotecas, projetos *Open Source* usados em múltiplos sistemas
  - vários *vendors* tendo que coordenar *advisories*
- Esta complexidade que está gerando a demanda por *SBOM – Software Bill of Materials*



Fonte: FIRST Guidelines and Practices for Multi-Party Vulnerability Coordination and Disclosure
https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1

CVD já está Incorporado em Diversos Padrões

- ISO/IEC 29147 and 30111
  https://webstore.ansi.org/standards/iso/isoiec30111129147security
- EthicsfIRST
  https://ethicsfirst.org/
- FIRST PSIRT and CSIRT Services Frameworks
  https://www.first.org/standards/frameworks/
- Políticas da OECD e da União Europeia
  https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0482
  https://www.enisa.europa.eu/news/enisa-news/coordinated-vulnerability-disclosure-policies-in-the-eu
- IETF security.txt – *RFC 9116: A File Format to Aid in Security Vulnerability Disclosure*
  https://securitytxt.org
- Ato nº 77 da Anatel, Requisitos de Segurança Cibernética para Equipamentos para Telecomunicações, seção 6.1.6
  https://informacoes.anatel.gov.br/legislacao/atos-de-certificacao-de-produtos/2021/1505-ato-77

VDP – Vulnerability Disclosure Policy/Program

Política

- Definir regras claras e expectativas sobre como notificações de vulnerabilidades serão tratadas
  - tempos, mitigações, divulgação
- Facilitar o recebimento de notificações de vulnerabilidades que não seriam conhecidas
- Incentivar comportamento ético de pesquisadores de boa fé

Programa

- Um processo parte do Programa de Gestão de Riscos
- Pode ou não envolver Bug Bounty
- Se tiver Bug Bounty
  - forneça canais claros de comunicação
    - tenha pelo menos no seu *site* o `/.well-known/security.txt`
  - divulgue a política
  - seja explícito sobre
    - o que pode ou não fazer
    - o escopo do programa

Recomendações

Assuma o Controle da Priorização da Aplicação de Patches

Quem assume o risco, em última instância, é você e sua organização

- Não use apenas CVSS como critério
- Cobre seu fornecedor
  - Desconfie se a resposta for muito simplista
  - É OK ter uma solução própria, mas é necessário saber algo sobre quais métricas são usadas
  - Verifique se ele já não integra EPSS e/ou SSVC
- Complemente com sua própria avaliação
  - Os dados são todos públicos

Independente de ter uma Política ou Programa de Divulgação de Vulnerabilidades, tenha o
`https://<seu-site>/.well-known/security.txt`

`https://securitytxt.org/`

Outras Referências

- CVE/FIRST VulnCon 2024 & Annual CNA Summit
  Slides: https://www.first.org/conference/vulncon2024/program
  Vídeos: https://youtube.com/playlist?list=PLBAUUhONOrO_aB01lOv6XNRTHD4ueFVTp&feature=shared
- The Common Security Advisory Framework (CSAF)
  https://csaf.io/
- The Vulnerability Exploitability eXchange (VEX)
  https://www.ntia.gov/files/ntia/publications/vex_one-page_summary.pdf
- CIRCL Vulnerability Lookup Tool – facilitates quick correlation of vulnerabilities from various sources, independent of vulnerability IDs, and streamlines the management of Coordinated Vulnerability Disclosure (CVD).
  https://github.com/cve-search/vulnerability-lookup
- CERT.br – Estatísticas de notificações de dispositivos com serviços potencialmente vulneráveis expostos na Internet
  https://stats.cert.br/vulns/

Obrigada

@ cristine@cert.br

@ Notificações para: cert@cert.br 𝕏 @certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br