O mundo roda em *software* vulnerável. Como melhorar o cenário?

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

24º Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais
São José dos Campos, SP – 19 de setembro de 2024

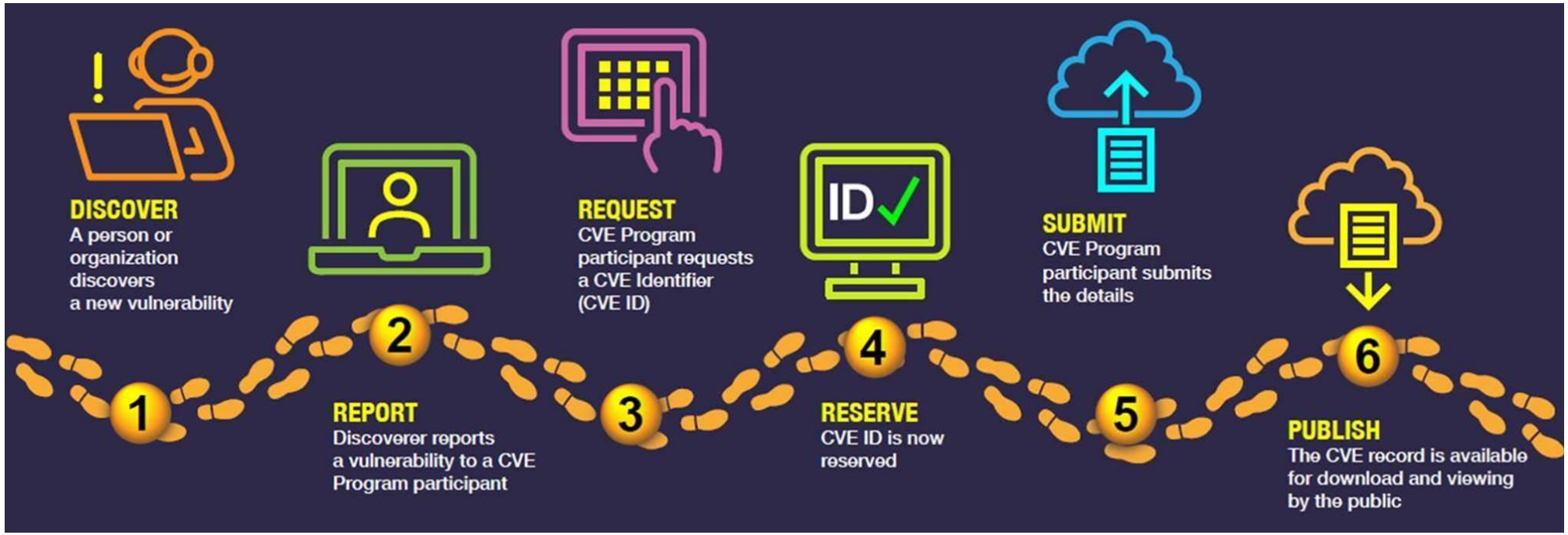
cert.br nic.br cgi.br

CVE – Common Vulnerabilities and Exposures:
“Ou tem CVE ou não existe”

TLP:CLEAR

“*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*.”

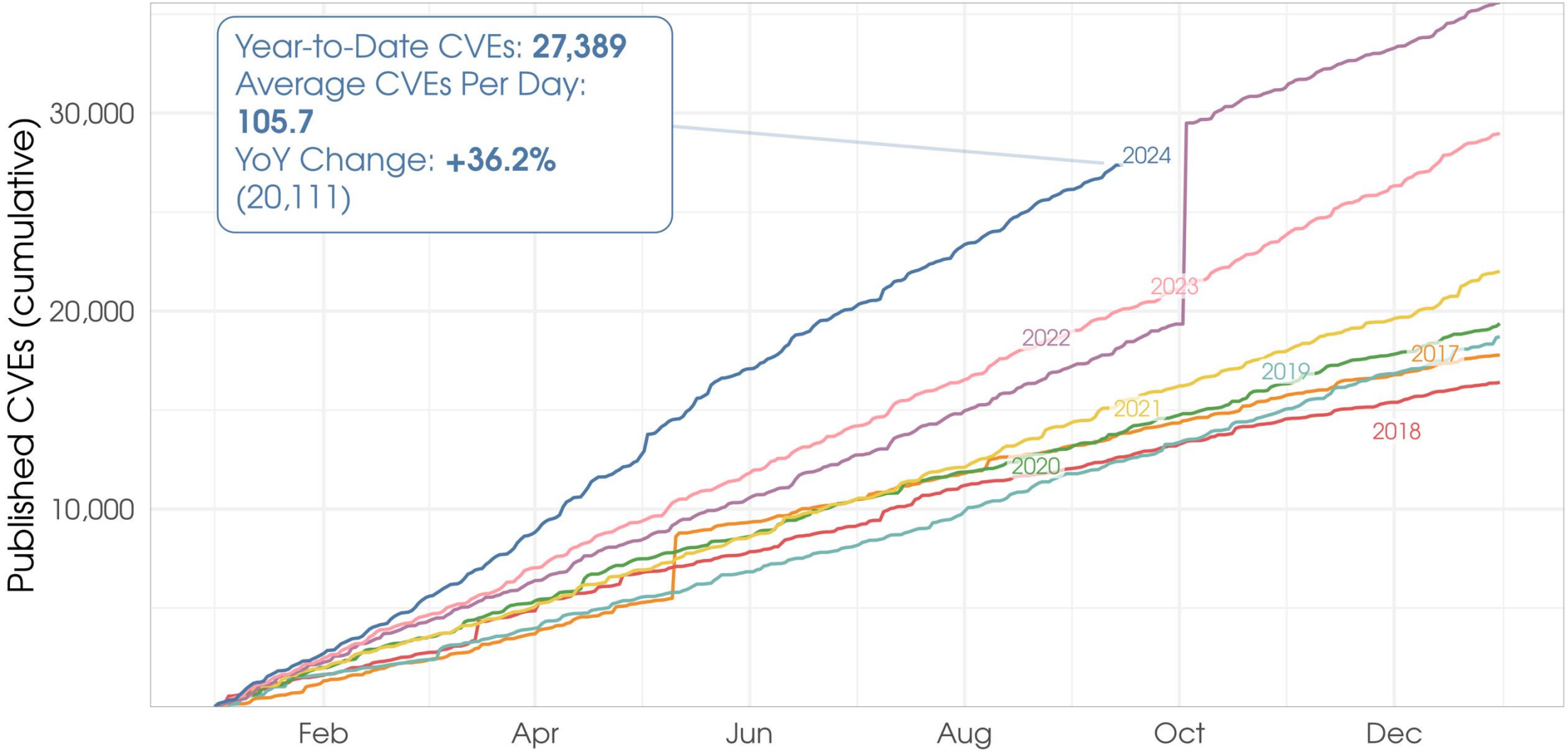


https://www.cve.org/About/Process

TLP:CLEAR

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

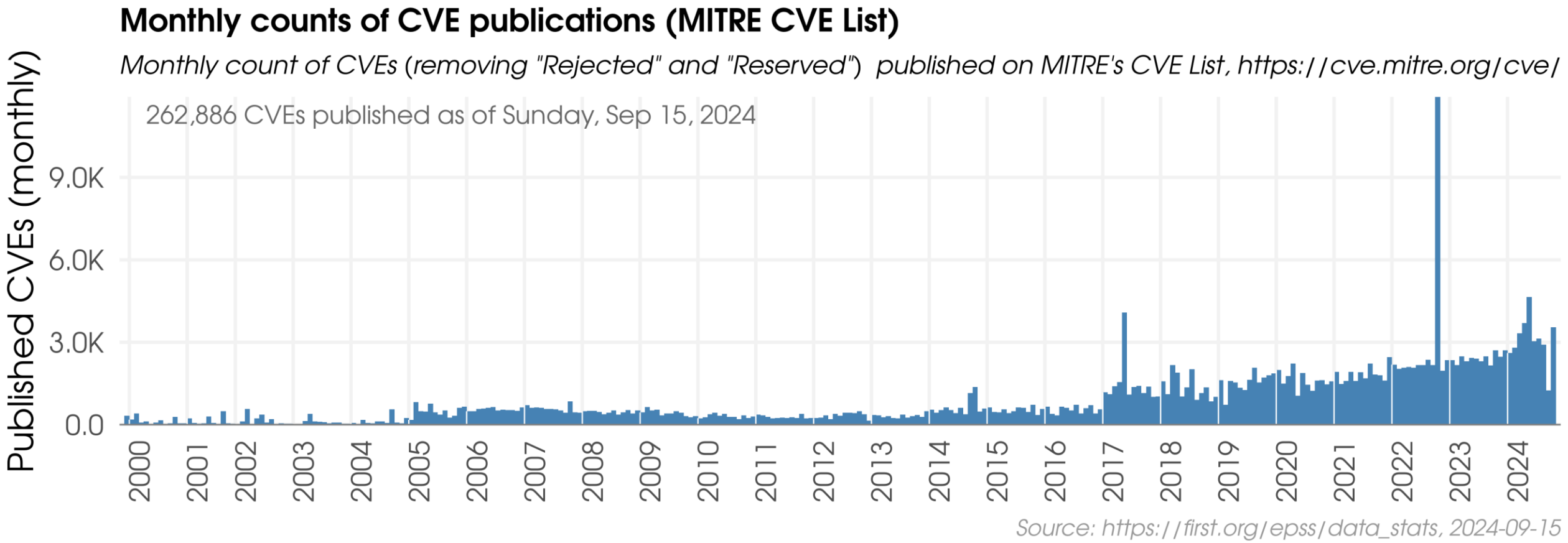
Lines showing the daily cumulative count of published CVEs on MITRE's CVE List, https://cve.mitre.org/cve/



Source: https://first.org/epss/data_stats, 2024-09-15

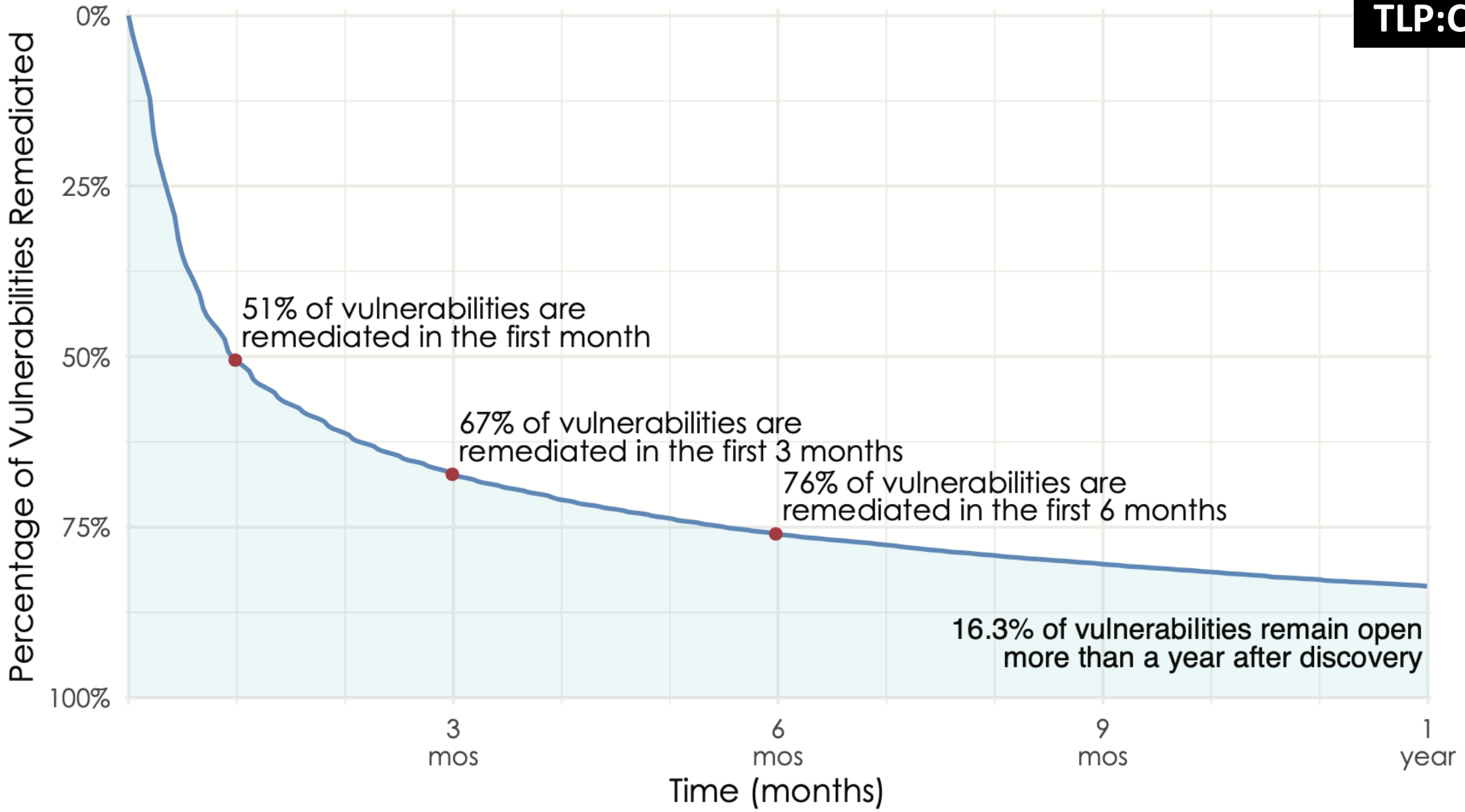
Fonte: https://www.first.org/epss/data_stats

TLP:CLEAR



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

TLP:CLEAR



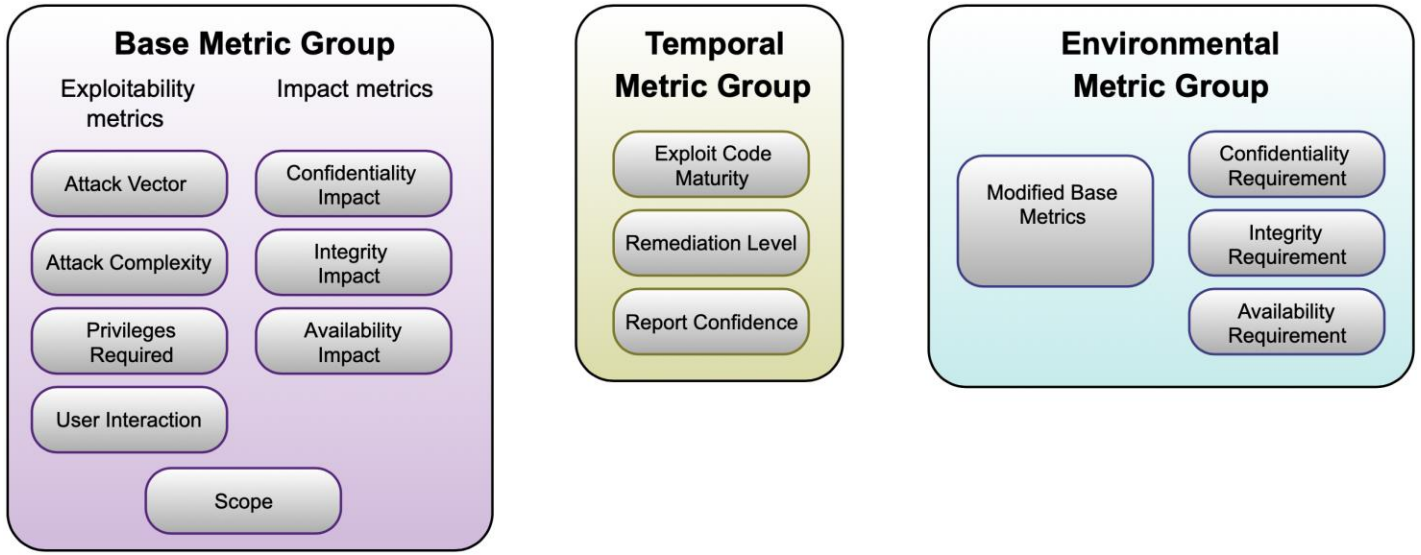
Fonte: https://www.cyentia.com/patching-fast-and-slow/ | https://www.cyentia.com/why-your-mttr-is-probably-bogus/

CVSS v3.1

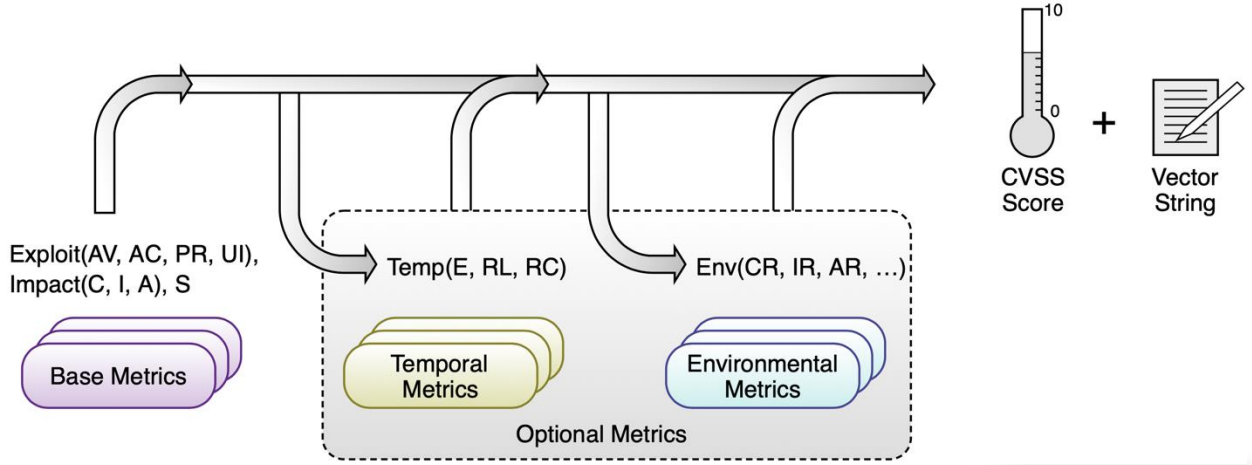
TLP:CLEAR

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

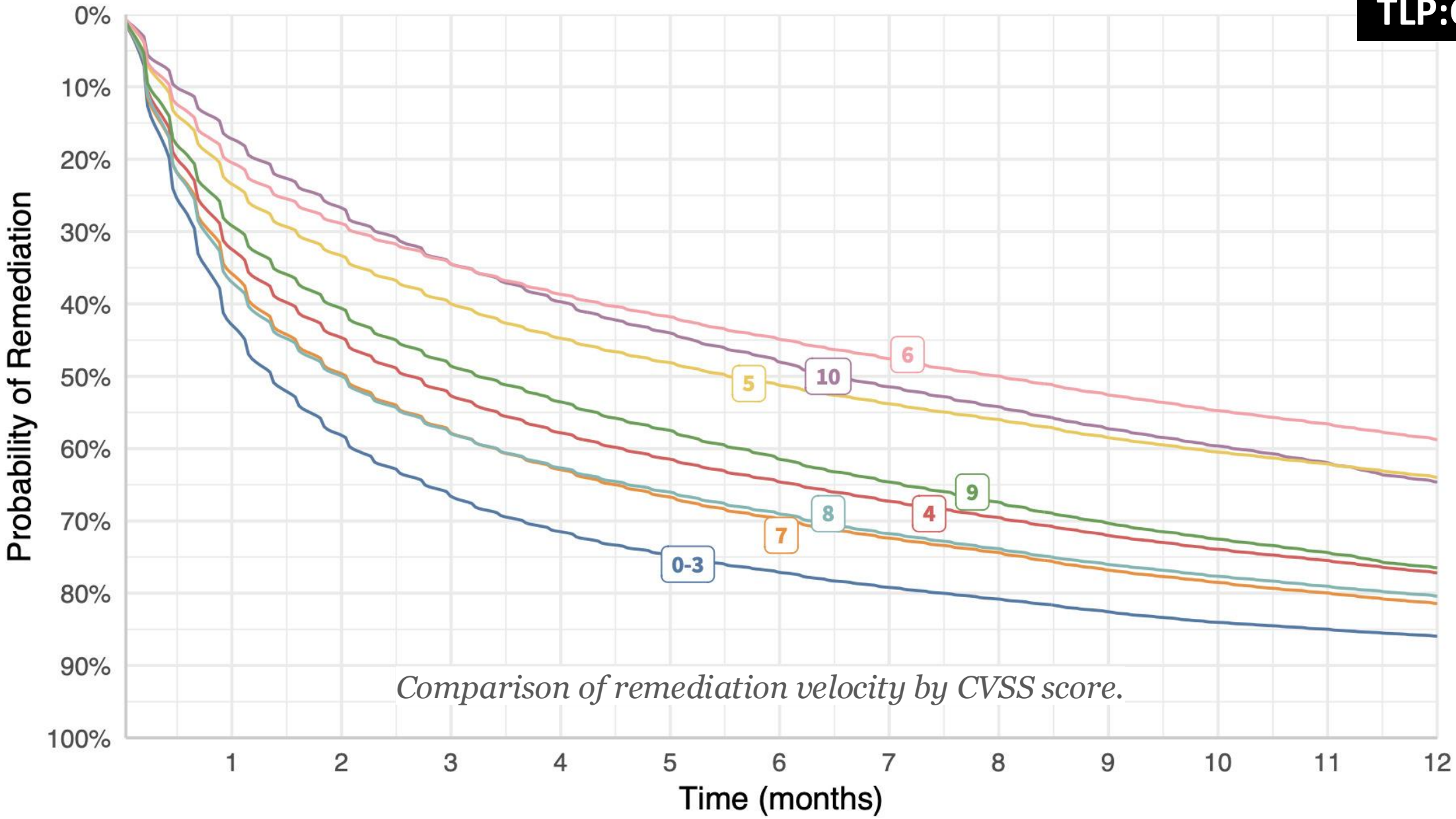
CVSS Metric Groups



CVSS Metrics and Equations

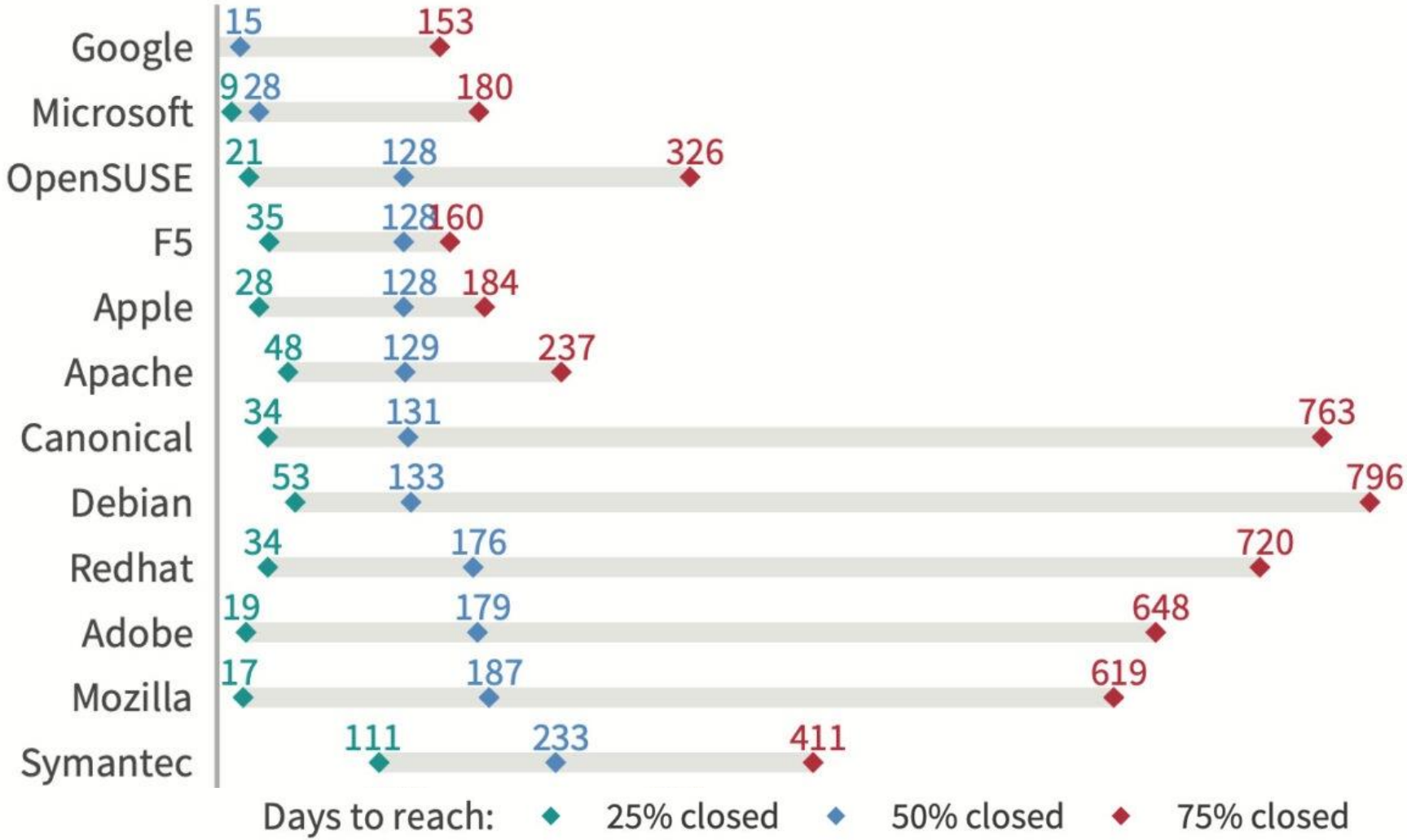


Fonte: https://www.first.org/cvss/



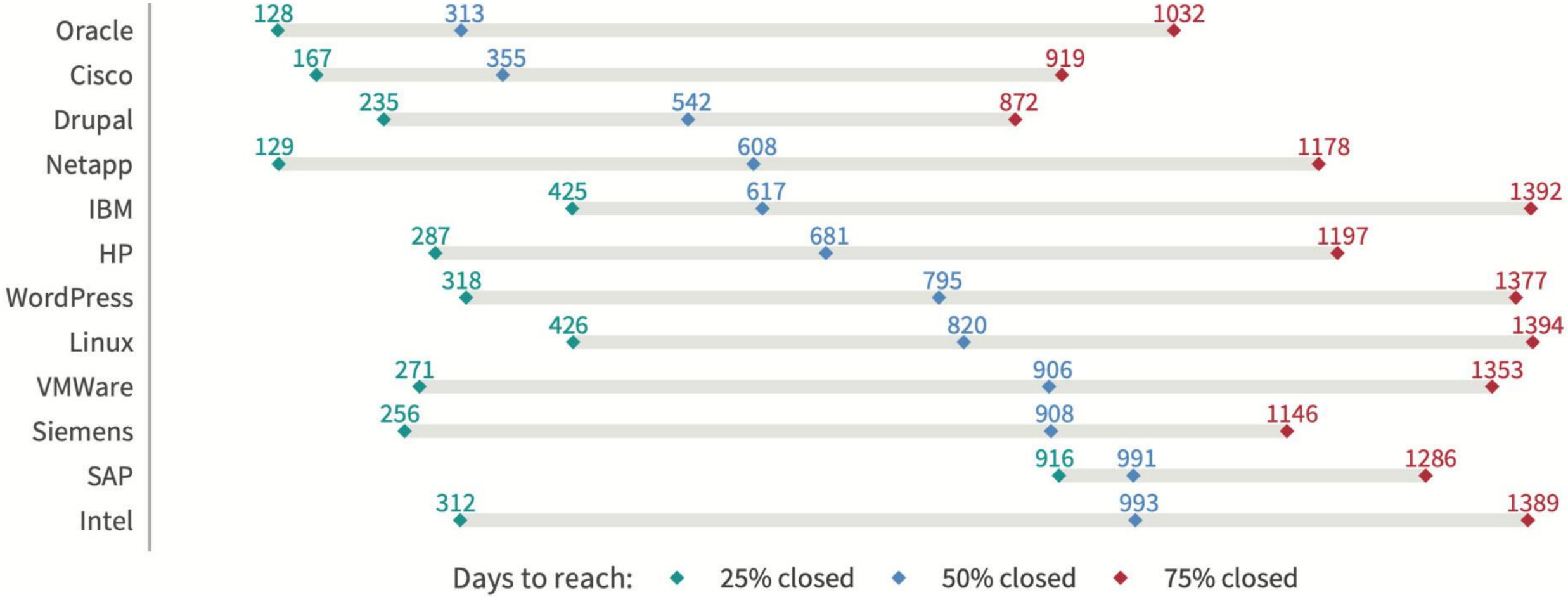
Comparison of remediation velocity by CVSS score.

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



Comparing remediation velocity for major product vendors (1/2)

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



Comparing remediation velocity for major product vendors (2/2)

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

Algumas Estatísticas Globais

- **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**
- 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

Algumas Estatísticas Nacionais

"Este artigo investiga o problema do *software* desatualizado em organizações"

- mais de 129 milhões de registros
- 23 mil usuários
- 567 organizações."

Proporção de *Software* Desatualizado

– Usuários passaram 65% do tempo usando *software* desatualizado

– 89% dos usuários usaram pelo menos uma vez *software* desatualizado há um ano ou mais

Tempo de Desatualização

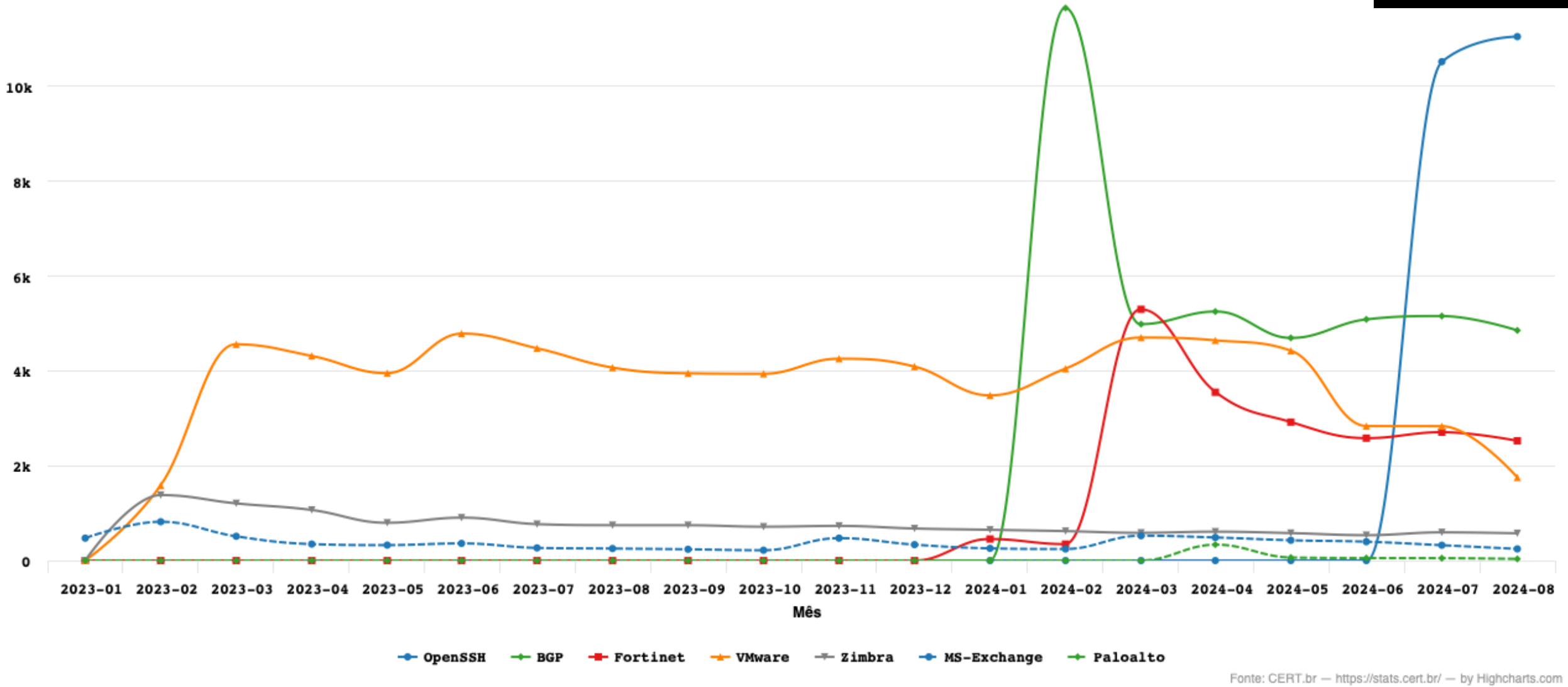
– 37% → uso de software desatualizado <= 3 meses

– 24% → uso de software desatualizado >= 12 meses

– 4% das horas gastas com navegadores → versões >= 12 meses obsoletas!

Fonte:
Obsolescência não-Programada: Análise do Uso de *Software* Desatualizado em Ambiente de Produção
Luan Marko Kujavski, Ulisses Penteado, Paulo Lisboa de Almeida, André Grégio, SBSeg 2024
https://sol.sbc.org.br/index.php/sbseg/article/view/30046/29853

TLP:CLEAR



Notificações feitas pelo CERT.br, de dispositivos com serviços potencialmente vulneráveis expostos na Internet

Fonte: https://stats.cert.br/vulns/

Divulgação de Informações Sobre Vulnerabilidades

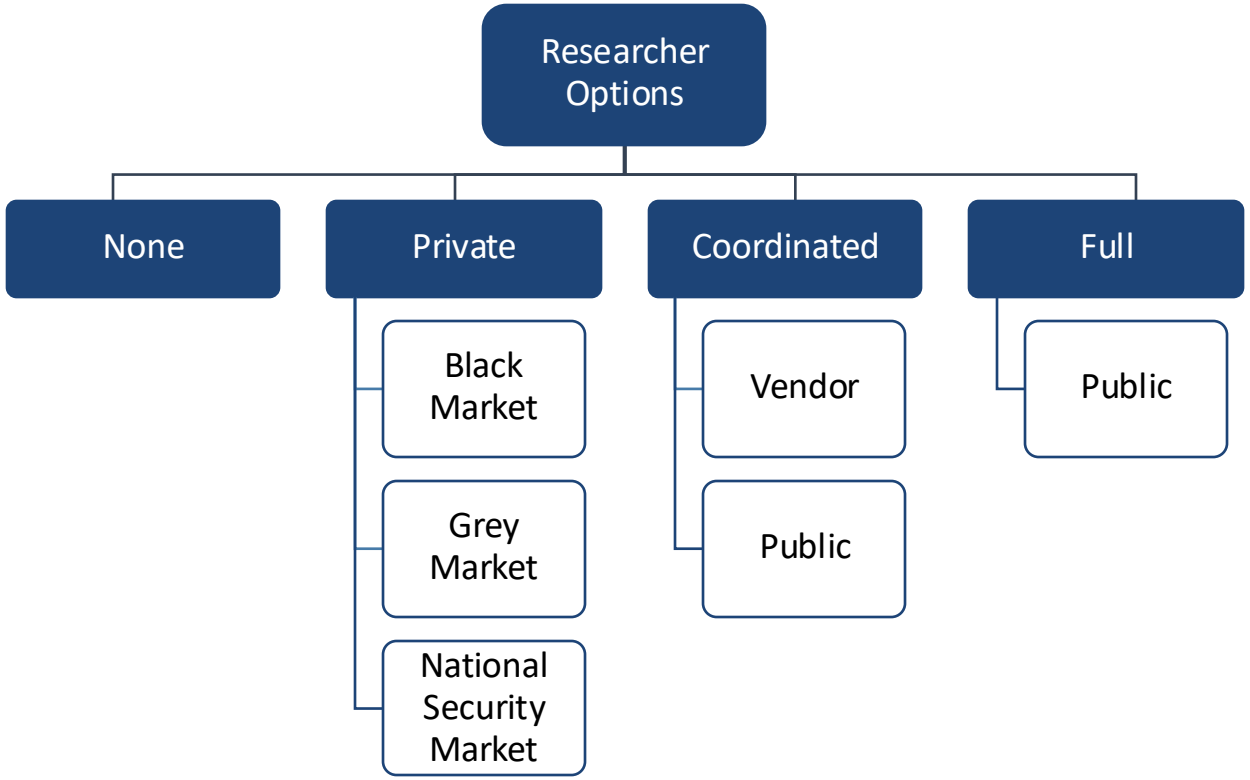
Opções de divulgação de quem descobre uma vulnerabilidade:

– Esconder a existência

– Vender para uma entidade privada
  - Crime organizado
  - Fornecedores de *spyware* comercial
    - como Zerodium, Aglaya e DarkMatter
  - Governos

– Optar por divulgação coordenada
  - Fabricante, CERT de Coordenação, programa de Bug Bounty, etc.

– Divulgar imediatamente de forma pública



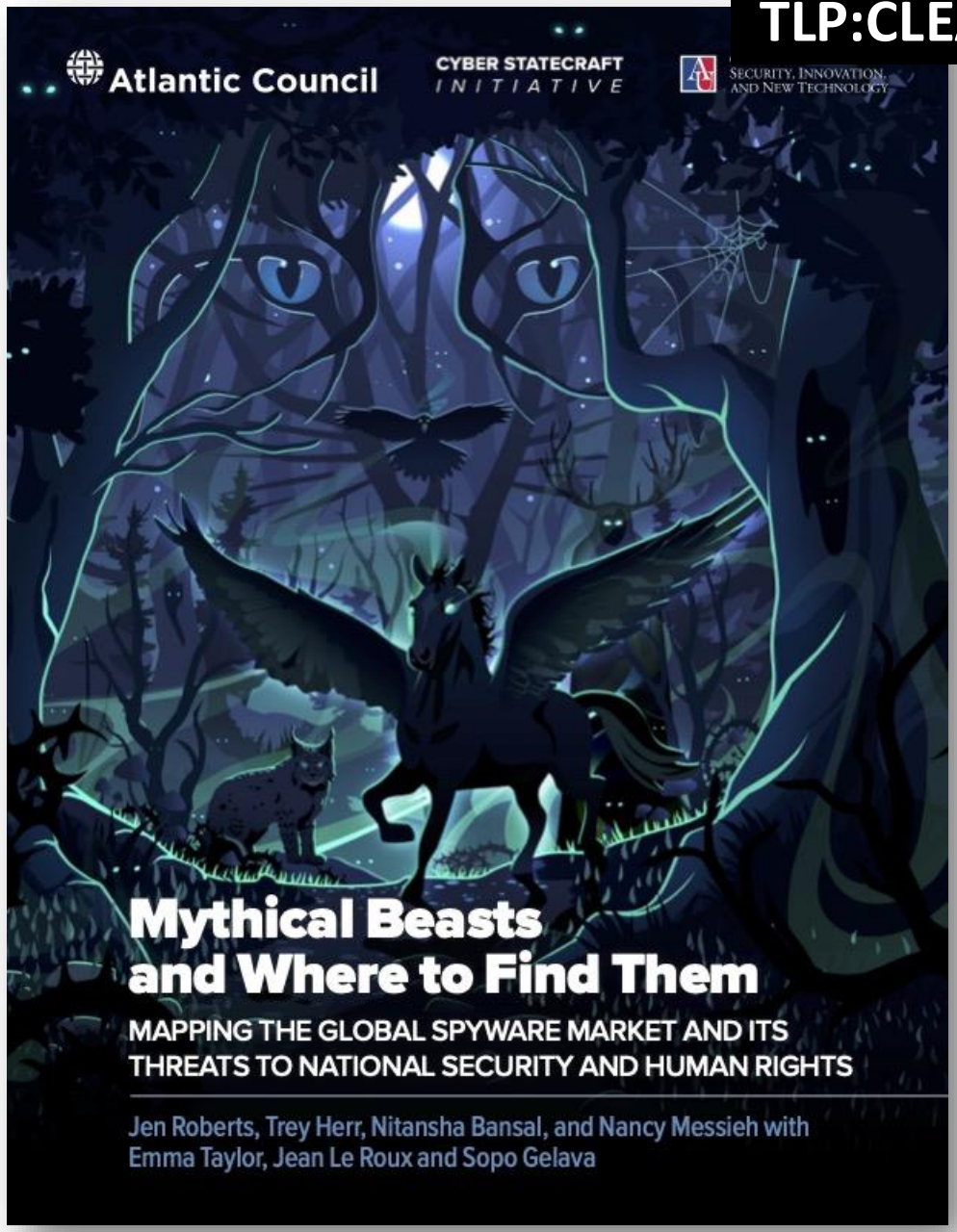
TLP:CLEAR

Mercado Global de *Spyware* e Zero-Days

- Out of 195 countries in the world, at least **80** are known to **have procured spyware** from commercial vendors.
- 14 of the 27 countries in the European Union have **purchased spyware** from just one vendor, the **NSO Group**.
- **Spyware vendors** were attributed to **50% of all zero-day exploits** discovered by one company's threat research team in 2023, including **64% of all exploits in mobile and browser** software.

"Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and its Threats to National Security and Human Rights"

https://dfrlab.org/2024/09/04/mythical-beasts-and-where-to-find-them-report/



Como melhorar o cenário?

cert.br nic.br cgi.br


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

Gestão de Vulerabilidades

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

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

Priorização de *Patches* com Base em Risco

Risco = Vulnerabilidade + Ameaça + Impacto

Queremos responder essa pergunta:

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?

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

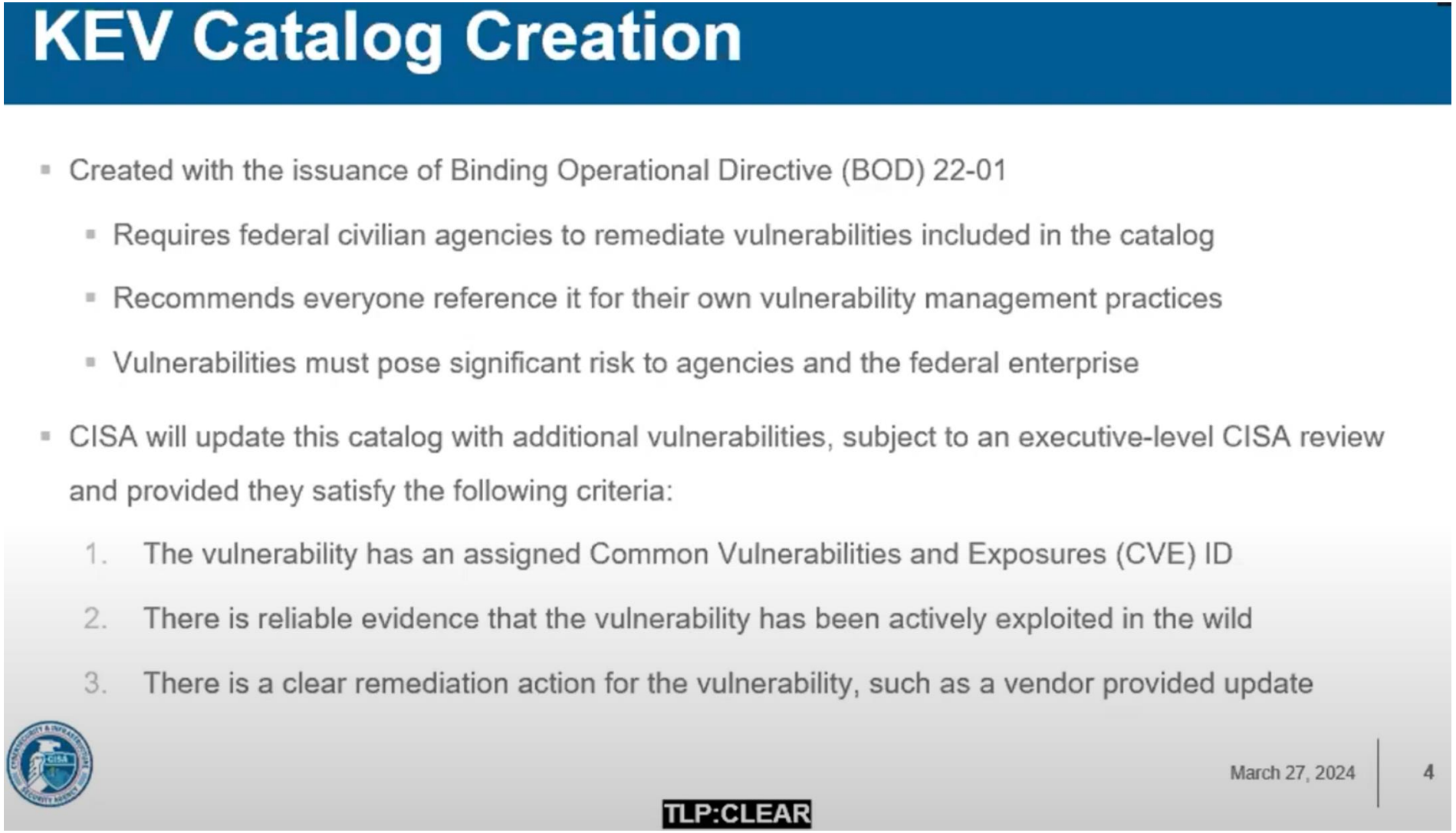
– **Probabilidade de** uma vulnerabilidade **ser ativamente explorada** nos próximos 30 dias

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
  - CISA criou a base KEV (Known Exploited Vulnerabilities) como parte deste esforço

CISA KEV – *Known Exploited Vulnerabilities*

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

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

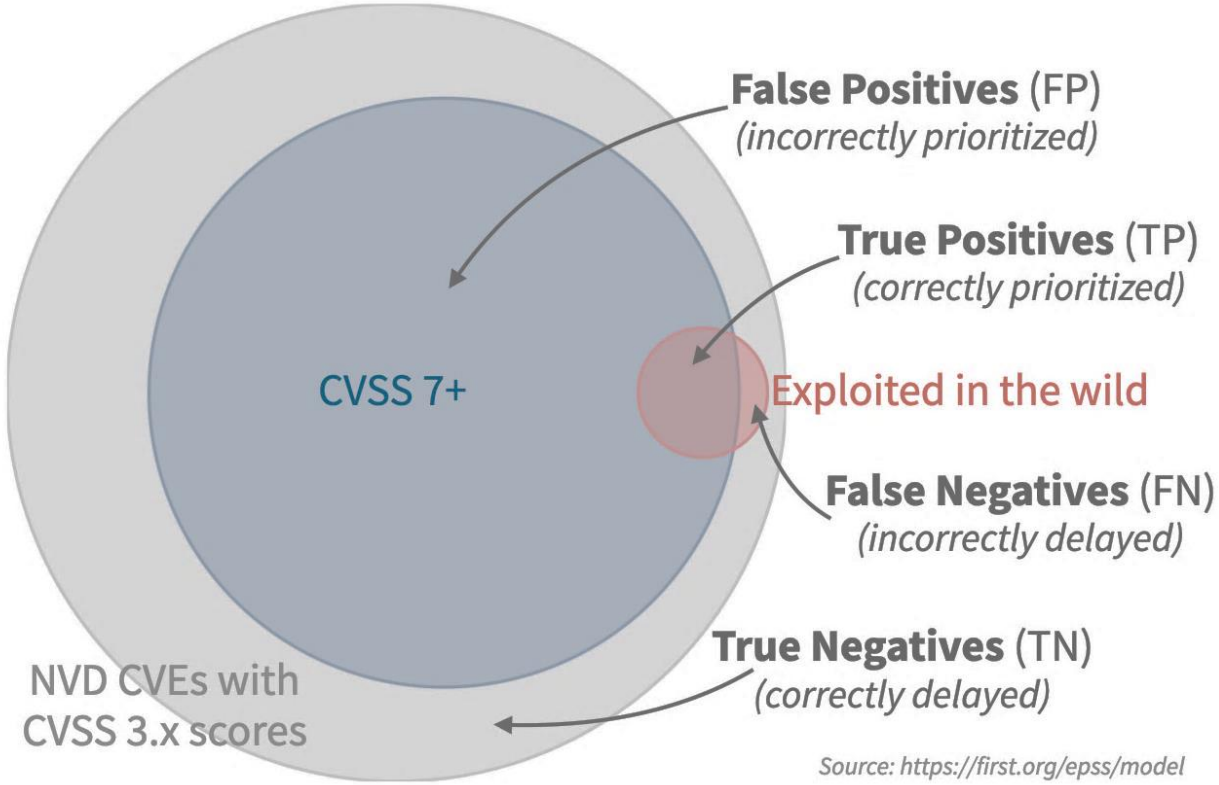
– Dados completos – arquivo CSV atualizado diariamente:
  - https://www.first.org/epss/data_stats

Efetividade do EPSS na Vida Real

Metodologia

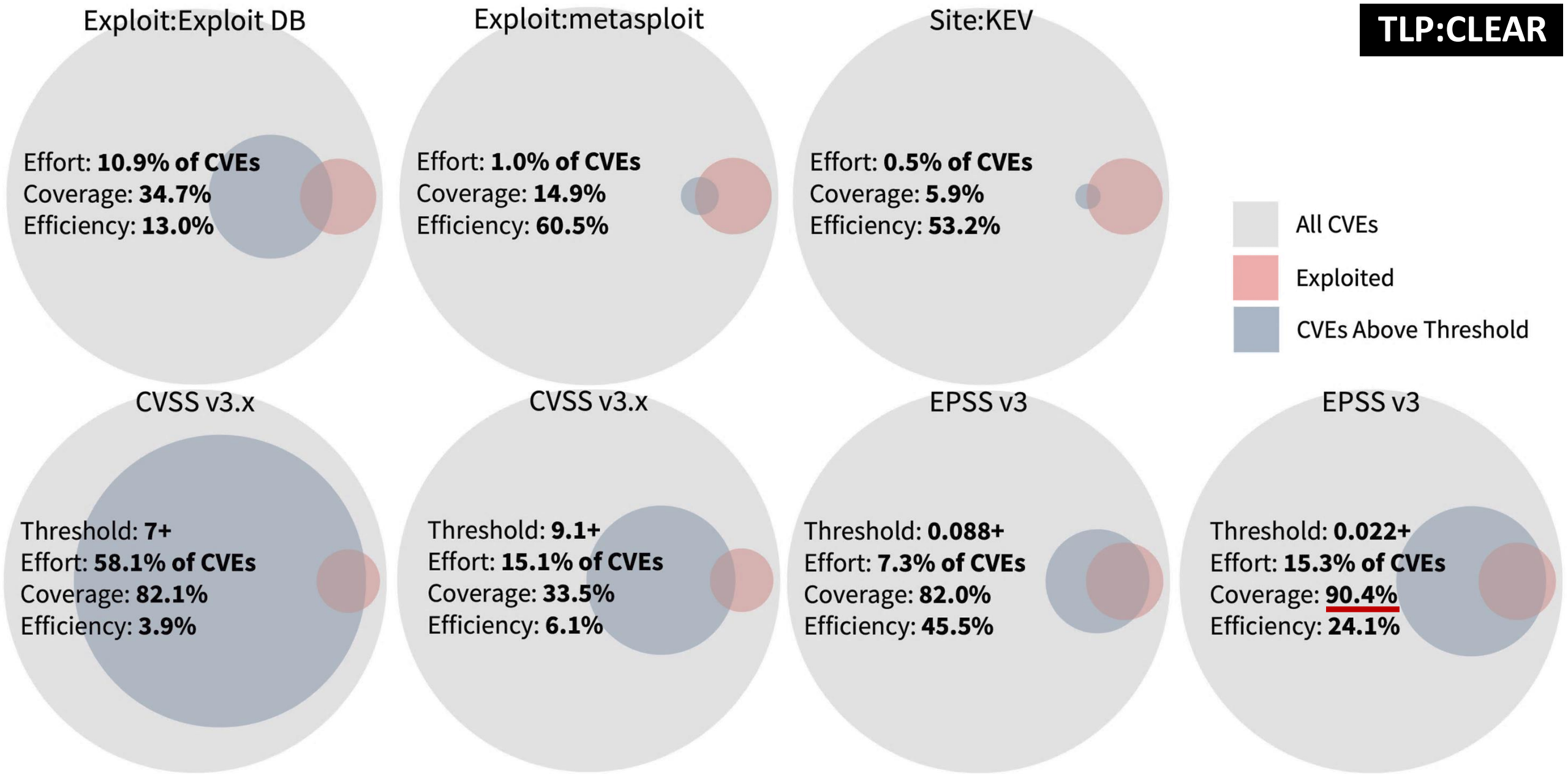
- 1 ano de dados usados para treinar o modelo
  - CVEs publicados entre 01/11/2021 – 31/10/2022
- Período de teste: dezembro/2022
- Avaliar para este mês
  - predições do EPSS versus
  - outras estratégias de priorização

Entendendo os Gráficos do próximo *slide*



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

TLP:CLEAR



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

CVSS COMMON VULNERABILITY SCORING SYSTEM + KEV e EPSS Exploit Prediction Scoring System + SSVC

CVD, VDP & Bug Bounties

cert.br nic.br cgi.br

TLP:CLEAR

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

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

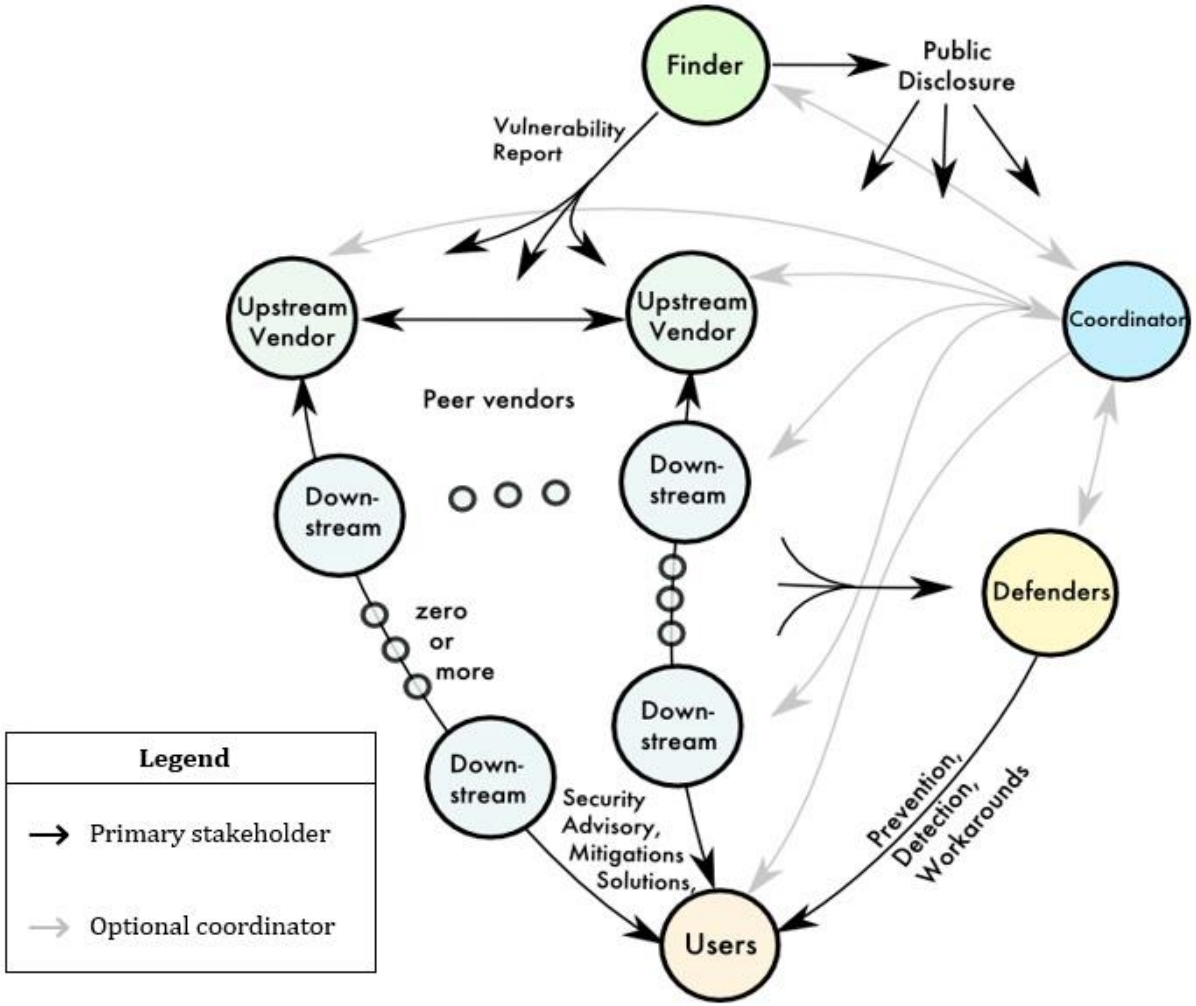
– Melhorar processos

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:
  - vários *vendors* tendo que coordenar *advisories*
  - exemplo: bibliotecas e projetos *Open Source* usados em múltiplos sistemas
- 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

Falando em SBOM

Software Bill of Materials (SBOM)

- a nested inventory, a list of ingredients that make up software components
- identifies and lists software components, information about those components, and supply chain relationships between them

Software composition analysis (SCA)

- SCA tools identify all open source packages in an application and all the known vulnerabilities of those packages.
- Software composition analysis tools can also be used to generate a software bill of materials (SBOM or software BOM) that includes all the open source components used by an application.

Vulnerability Exploitability eXchange (VEX)

- a form of a security advisory that indicates whether a product is affected by a known vulnerability or vulnerabilities
- can support more effective use of SBOM data
- VEX documents are machine readable. The goal is to support greater automation across the vulnerability ecosystem, including disclosure, vulnerability tracking, and remediation

OASIS Common Security Advisory Framework (CSAF)

- a language to exchange Security Advisories
- automate the creation and consumption of security vulnerability information and remediation.

Referências sobre SBOM, VEX e CSAF

- CSAF & VEX in 4 minutes: https://youtu.be/vQ_xY3lmZOc
- https://www.cisa.gov/sbom
- https://www.cisa.gov/resources-tools/resources/sbom-faq
- https://www.ntia.gov/files/ntia/publications/framingsbom_20191112.pdf
- https://english.ncsc.nl/publications/publications/2021/february/4/using-the-software-bill-of-materials-for-enhancing-cybersecurity
- https://www.enisa.europa.eu/publications/cyber-resilience-act-requirements-standards-mapping/@@download/fullReport
- https://www.cisa.gov/resources-tools/resources/when-issue-vex-information
- https://www.amazon.com/Software-Supply-Chain-Security-End/dp/1098133706/
- https://csaf.io/
- https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/CSAF/CSAF_node.html

CVD já está Incorporado em Diversos Padrões

- ISO/IEC 29147 and 30111
  https://webstore.ansi.org/standards/iso/isoiec3011129147security
- 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

Organizações em Geral Devem Considerar Ter:
VDP – Vulnerability Disclosure Policy/Program

TLP:CLEAR

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`** https://securitytxt.org
  - divulgue a política
  - seja explícito sobre
    - o que pode ou não fazer
    - o escopo do programa

Pesquisa de Vulnerabilidades com Ética e Dentro da Lei

"Não é porque dá pra fazer
que se deve fazer."

- É importante pesquisar vulnerabilidades e como sistemas podem ser invadidos
- Mas o objetivo **DEVE** ser corrigir e proteger
  - Procure participar de um processo de CVD
  - Se não encontrar, procure
    - um CERT/CSIRT que faça CVD
    - uma plataforma séria de Bug Bounty
- Academia deve incentivar pesquisa responsável de segurança ofensiva
  - Conferências como Usenix Security e WOOT (Conference on Offensive Technologies) só aceitam publicar artigos se foi seguido CVD

Lei 12.737

"Art. 154-A. **Invadir** dispositivo informático alheio, conectado ou não à rede de computadores, **mediante violação** indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações **sem autorização expressa ou tácita do titular** do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa."

TLP:CLEAR

Pesquisadores de Vulnerabilidades

- Informar-se sobre a complexidade do processo de CVD
- Seguir as regras
  - CVD ("responsible disclosure")
  - Bug Bounty
- Encontrar vulnerabilidades é crucial
  - dentro da lei
  - sem dar vantagens aos atacantes
  - dando tempo de todos os fabricantes lançarem correções ou mitigações

Empresas Produtoras de *Software*

- Institucionalizar
  - CVD
  - PSIRT
- Implementar **seriamente** processos de desenvolvimento seguro de *software*
  - SSDLC / Dev**Sec**Ops
- Publicar suas políticas
  - CVD
  - Bug Bounty
- Manter o SBOM (*Software Bill of Materials*)

Organizações Usuárias de *Software*

- Priorizar melhor aplicação de patches
  - CVSS não é métrica de Priorização!
  - Não dependa somente de uma solução comercial
- Olhar para outras métricas e *frameworks*
  - KEV / EPSS / SSVC
- Deixar mais claras as regras para quem encontrar vulnerabilidades
  - VDP
  - Bug Bounty
  - **`security.txt`**

Reflexões Finais

cert.br nic.br cgi.br

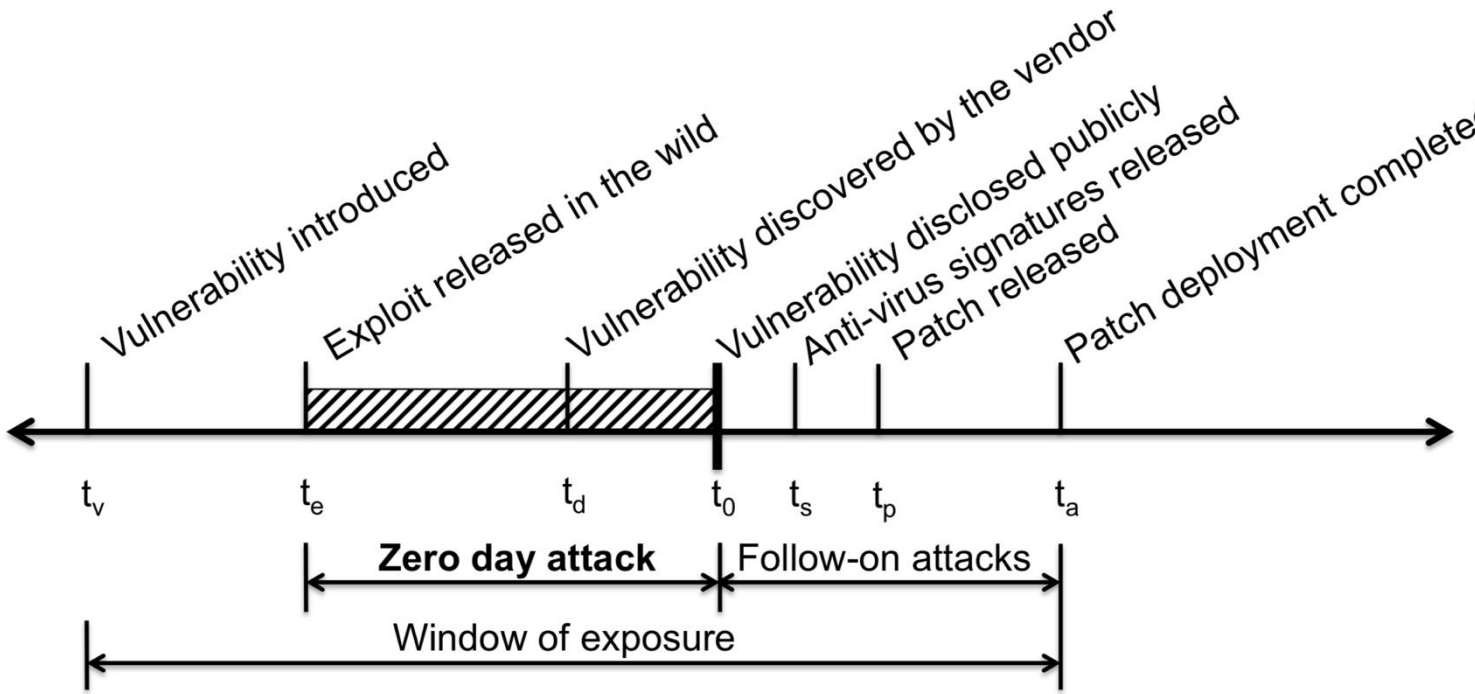
Conseguimos proteger nossos sistemas?
Responsible Disclosure vs. Stock Pilling Vulnerabilities

Desafios no cenário

- Vulnerabilidades descobertas pelos governos e mantidas em “segredo”
- Mercado de compra e venda de *zero days*
  - Governos são os principais compradores dos *brokers* legítimos
  - “Pesquisadores” tendem a vender para quem pagar mais
  - Programas de *Bug Bounty* dos fabricantes não conseguem competir

➢ Dura verdade: **só há patches se o fabricante conhece a vulnerabilidade, fora isso, todos estamos vulneráveis**

Attack Timeline



Fonte: ***Before We Knew It: An Empirical Study of Zero-day Attacks in the Real World Proceedings of the 2012 ACM Conference on Computer and Communications Security***
http://doi.acm.org/10.1145/2382196.2382284

"*0-Days*" e governos estocando vulnerabilidades:
Do *EternalBlue* ao *WannaCry*

2012 (ou antes) – NSA descobre uma vulnerabilidade grave nos sistemas Windows, que permite comprometimento remoto. Dá o nome de *EternalBlue* e não divulga a ninguém.

1º Semestre de 2016 – um grupo chamado *The Shadow Brokers* ganha acesso a dados da NSA, que incluem diversas vulnerabilidades, entre elas o *EternalBlue*.

Agosto de 2016 – *The Shadow Brokers* começa a colocar publicamente na Internet algumas das ferramentas da NSA.

07 de janeiro de 2017 – *The Shadow Brokers* começa a vender algumas das ferramentas, incluindo o *EternalBlue*.

Janeiro/Fevereiro de 2017 – NSA contata a Microsoft com detalhes sobre a vulnerabilidade.

14 de março de 2017 – Microsoft lança a correção MS17-010, que corrige a vulnerabilidade identificada como CVE-2017-0144 – o *EternalBlue*.

Quem ainda usava os Windows antigos, não conseguia aplicar patches sem quebrar aplicações críticas

14 de abril de 2017 – O grupo *The Shadow Brokers* dilvulga 300MB de materiais da NSA no Github, incluindo o *EternalBlue*.

12 de maio de 2017 – Tem início a propagação do *Ransomware WannaCry* explorando o *EternalBlue*.

https://boot13.com/windows/timeline-nsa-hacking-tool-to-wannacry/
https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/

Divulgação de Informações Sobre Vulnerabilidades: **Precisamos Estimular Comportamento Responsável**

TLP:CLEAR

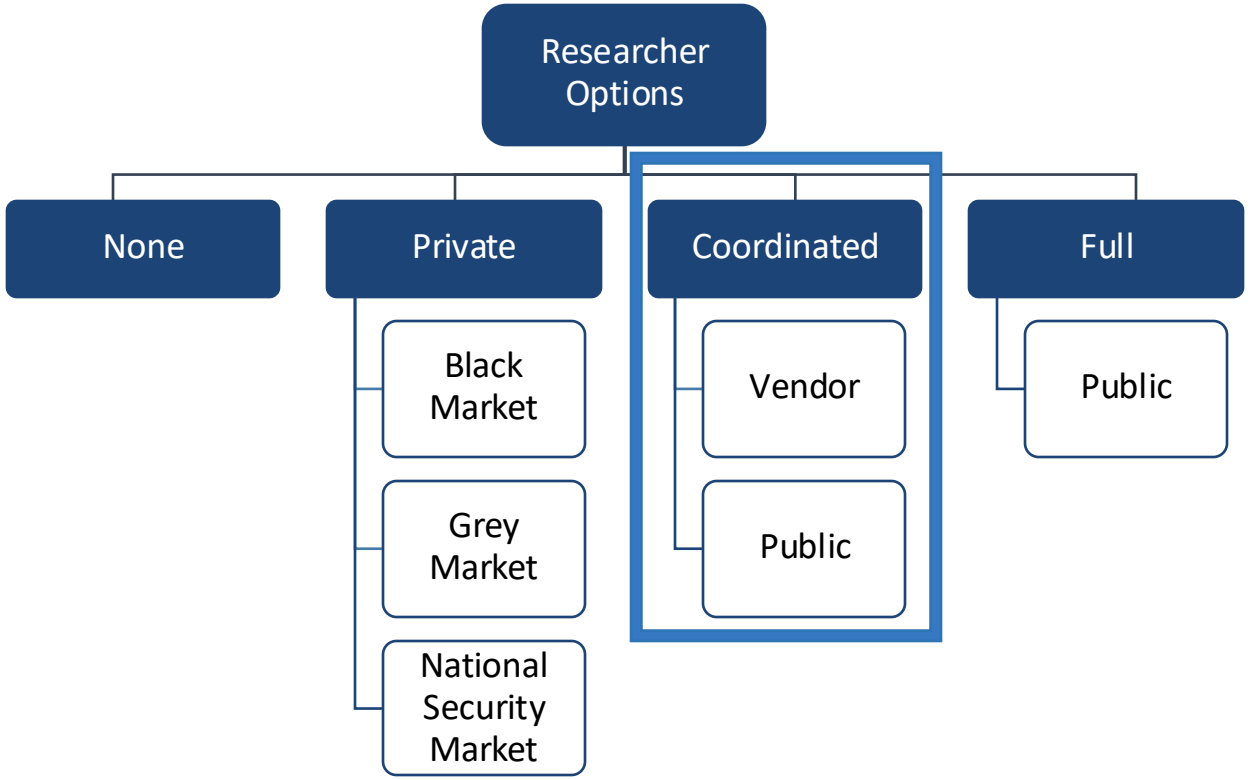
Opções de divulgação de quem descobre uma vulnerabilidade:

– Esconder a existência

– Vender para uma entidade privada
  - Crime organizado
  - Fornecedores de *spyware* comercial
    - como Zerodium, Aglaya e DarkMatter
  - Governos

– **Optar por divulgação coordenada**
  - **Fabricante, CERT de Coordenação, programa de Bug Bounty, etc.**

– Divulgar imediatamente de forma pública



TLP:CLEAR

Referências Adicionais

- 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
- PSIRT (Product Security Incident Response Team) Services Framework
  https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1
- CSIRT (Computer Security Incident Response Team) Services Framework
  https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
- 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 @certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br