nic.br cgi.br | cert.br

Grupo de Estudos do Setor de Telecomunicações
Exercício Guardião Cibernético 2021
20 de julho de 2021 | Evento *Online*

Gestão de vulnerabilidades além do básico – como utilizar os novos padrões para priorizar as ações

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

cert.br nic.br cgi.br

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CERT Nacional de Último Recurso

Serviços Prestados à Comunidade

Gestão de Incidentes

- Coordenação
- Análise Técnica
- Suporte à Mitigação e Recuperação

Consciência Situacional

- Aquisição de Dados
  - *Honeypots* Distribuídos
  - SpamPots
  - *Threat feeds*
- Compartilhamento das Informações

Transferência de Conhecimento

- Conscientização
  - Desenvolvimento de Boas Práticas
  - Cooperação, Eventos e Reuniões (*Outreach*)
- Treinamento
- Aconselhamento Técnico e Político

Filiações e Parcerias:

FIRST Improving Security Together MEMBER

ACCREDITED BY TI TRUSTED INTRODUCER

APWG RESEARCH PARTNER www.antiphishing.org

CARNEGIE MELLON UNIVERSITY SOFTWARE ENGINEERING INSTITUTE

SEI Partner Network

HN/P

Criação:

Agosto/1996: CGI.br publica o relatório "Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil"[1]

Junho/1997: CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório[2]

[1] https://cert.br/sobre/estudo-cgibr-1996.html | [2] https://nic.br/pagina/gts/157

Missão

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Público Alvo (*Constituency*)

Redes que utilizam recursos administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

Governança

Mantido pelo **NIC.br** – Núcleo de Informação e Coordenação do .br

- todas as atividades são sustentadas pelo registro de domínios .br

O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

- entidade multissetorial
- responsável por coordenar e integrar as iniciativas e serviços da Internet no País

https://cert.br/sobre/
https://cert.br/sobre/filiacoes/
https://cert.br/about/rfc2350/

Resumo sobre os Incidentes Observados pelo CERT.br: **Causas Mais Comuns de Invasões e Vazamentos de Dados**

Ataques mais reportados e mais observados em sensores:

- Força bruta de senhas em serviços protegidos só com conta e senha. Exemplos:
  - *e-mails* e serviços em nuvem
  - acesso remoto e gestão remota de ativos de rede e servidores
- Comprometimento via exploração de vulnerabilidades conhecidas
  - falta de aplicação de correções
  - erros de configuração
  - falta/falha de processos

Veja também: Principais Ataques na Internet: Dados do CERT.br
https://youtu.be/nHh8hHaomFE?t=714
https://cert.br/stats/

Mais de 80% dos incidentes seriam evitados se

- todas as correções (*patches*) fossem aplicadas
- houvesse mais atenção a erros e configurações
- todos os serviços tivessem 2FA/MFA

Estudo Setorial
Segurança digital: uma análise de gestão de risco em empresas brasileiras
https://cetic.br/pt/publicacao/seguranca-digital-uma-analise-de-gestao-de-risco-em-empresas-brasileiras/

Você teria um conselho para as empresas para reduzir o número de incidentes?

“Multifactor Everything”

-- Katie Moussouris (Luta Security, US)
https://youtu.be/4tuC32PlyJk

You weren't hacked because you lacked space-age network defenses. Nor because cyber-gurus picked on you. It's far simpler than that

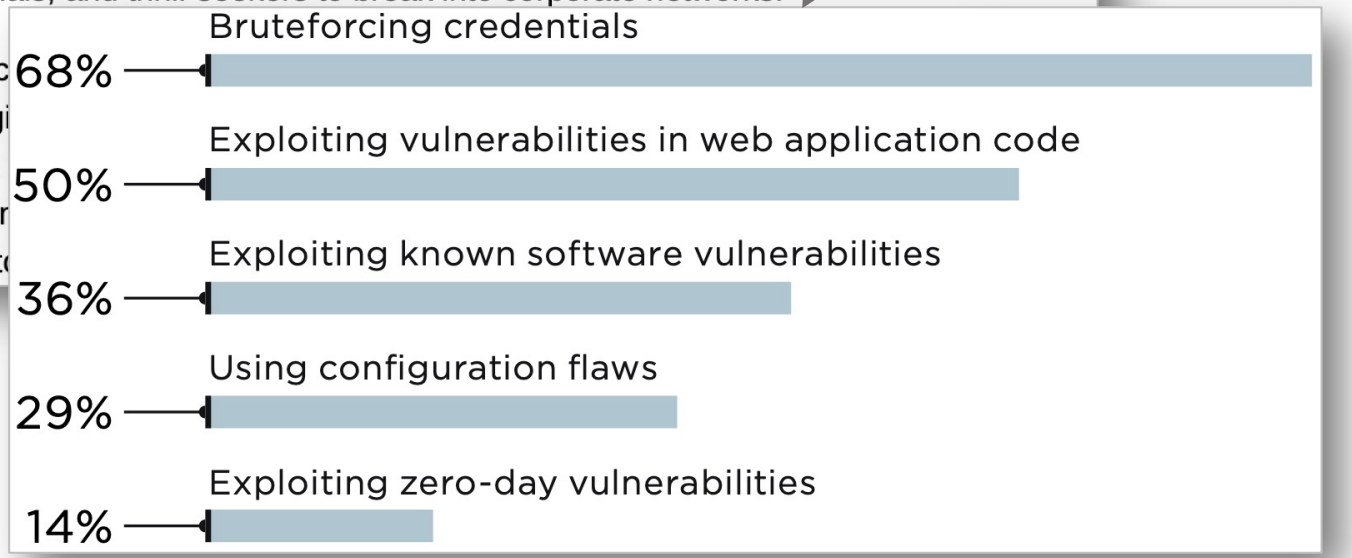
Three little words: Patches, passwords, policies

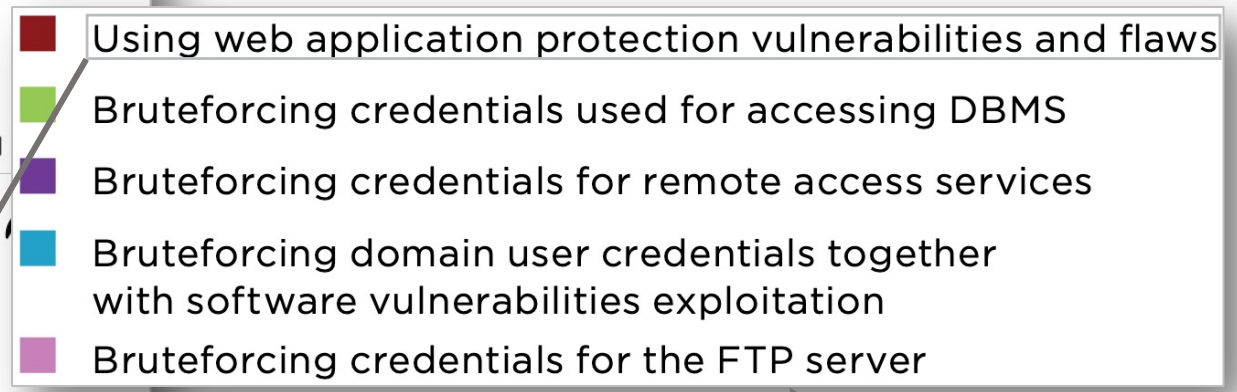
Thu 13 Aug 2020 // 07:06 UTC 31

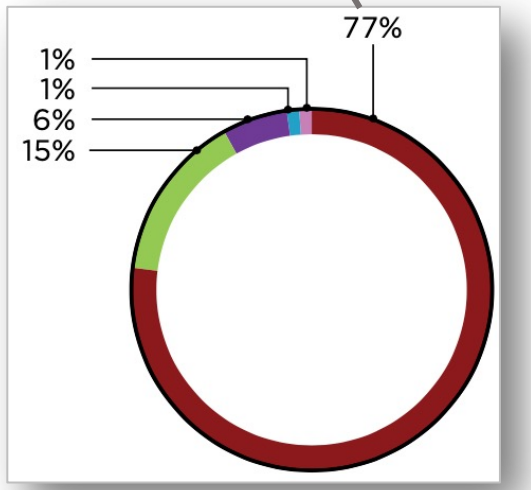
Shaun Nichols in San Francisco BIO EMAIL TWITTER

The continued inability of organizations to patch security vulnerabilities in a timely manner, combined with guessable passwords and the spread of automated hacking tools, is making it pretty easy for miscreants, professionals, and thrill-seekers to break into corporate networks.

This is acc
Technologi
and found
its red tear
available t







https://www.theregister.com/2020/08/13/pentest_networks_fail/
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/external-pentests-2020-eng.pdf

Gestão de Vulnerabilidades

cert.br nic.br cgi.br

CSIRT – Computer Security Incident Response Team

"*is an organizational unit (which may be virtual) or a capability that provides services and support to a defined constituency for preventing, detecting, handling, and responding to computer security incidents*"

Service Areas:

- Information Security Event Management
- Information Security Incident Management
- Vulnerability Management
- Situational Awareness
- Knowledge Transfer

PSIRT – Product Security Incident Response Team

"*an entity within an organization which, at its core, focuses on the identification, assessment and disposition of the risks associated with security vulnerabilities within the products*"

Service Areas:

- Stakeholder Ecosystem Management
- Vulnerability Discovery
- Vulnerability Triage and Analysis
- Remediation
- Vulnerability Disclosure
- Training and Education

https://www.first.org/standards/frameworks/

CSIRT – Computer Security Incident Response Team
Vulnerability Management Service Area

"*services related to the discovery, analysis, and handling of new or reported security vulnerabilities in information systems*"

- Vulnerability discovery / research
  - Identify a vulnerability that was exploited as part of a security incident
  - Learn about a new vulnerability from reading public sources or other third-party sources
    - sources can include vendor announcements, security websites, mailing lists, vulnerability databases, security conferences, social media, etc
  - Discover or search for new vulnerabilities as a result of deliberate activities or research
- Vulnerability report intake
- Vulnerability analysis
- Vulnerability coordination
- Vulnerability disclosure
- Vulnerability response
  - Actively take information about known vulnerabilities and act upon that information to prevent, detect, and remediate/mitigate those vulnerabilities
    - ✓ Vulnerability detection / scanning

      Actively engage in searching for the presence of known vulnerabilities in deployed systems.
    - ✓ Vulnerability remediation

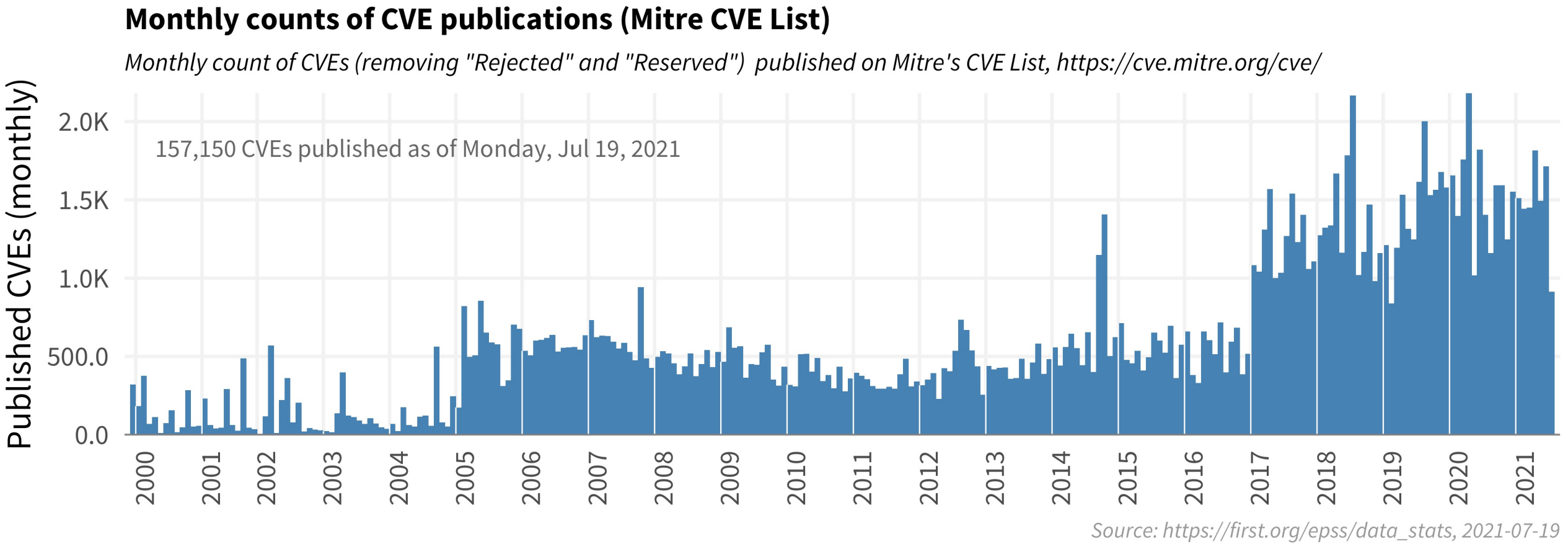
      Remediate or mitigate vulnerabilities to prevent them from being exploited, typically through the **timely application of vendor-provided patches or other solutions**.

https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1 - 7-Service-Area-Vulnerability-Management

Por que Pensar em Priorizar a Aplicação de Correções de Segurança

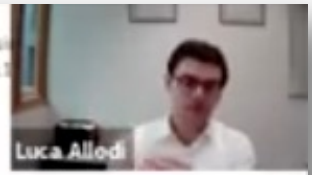
cert.br nic.br cgi.br

MITRE CVE (*Common Vulnerabilities and Exposures*): **Número Mensal de Vulnerabilidades Catalogadas**

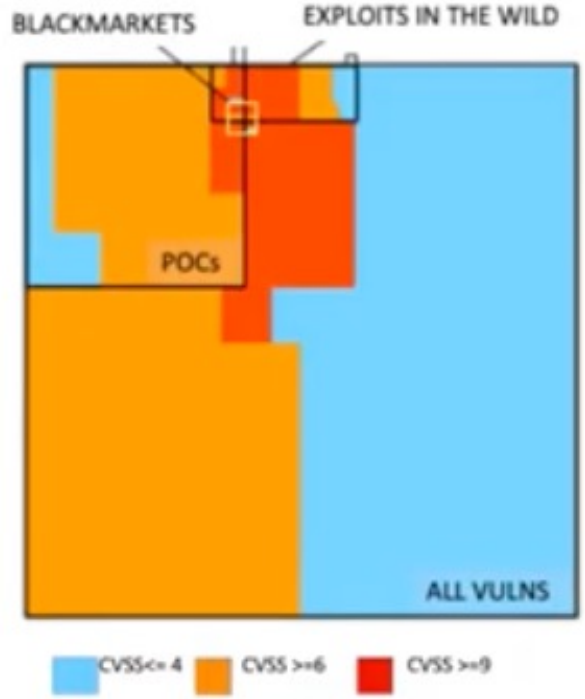


https://www.first.org/epss/data_stats

Luca Allodi and Fabio Massacci. 2014. Comparing Vulnerability Severity and Exploits Usi
Trans. Inf. Syst. Secur. 17, 1, Article 1 (August 2014), 20 pages. DOI https://doi.org/10.11



Where it all started..

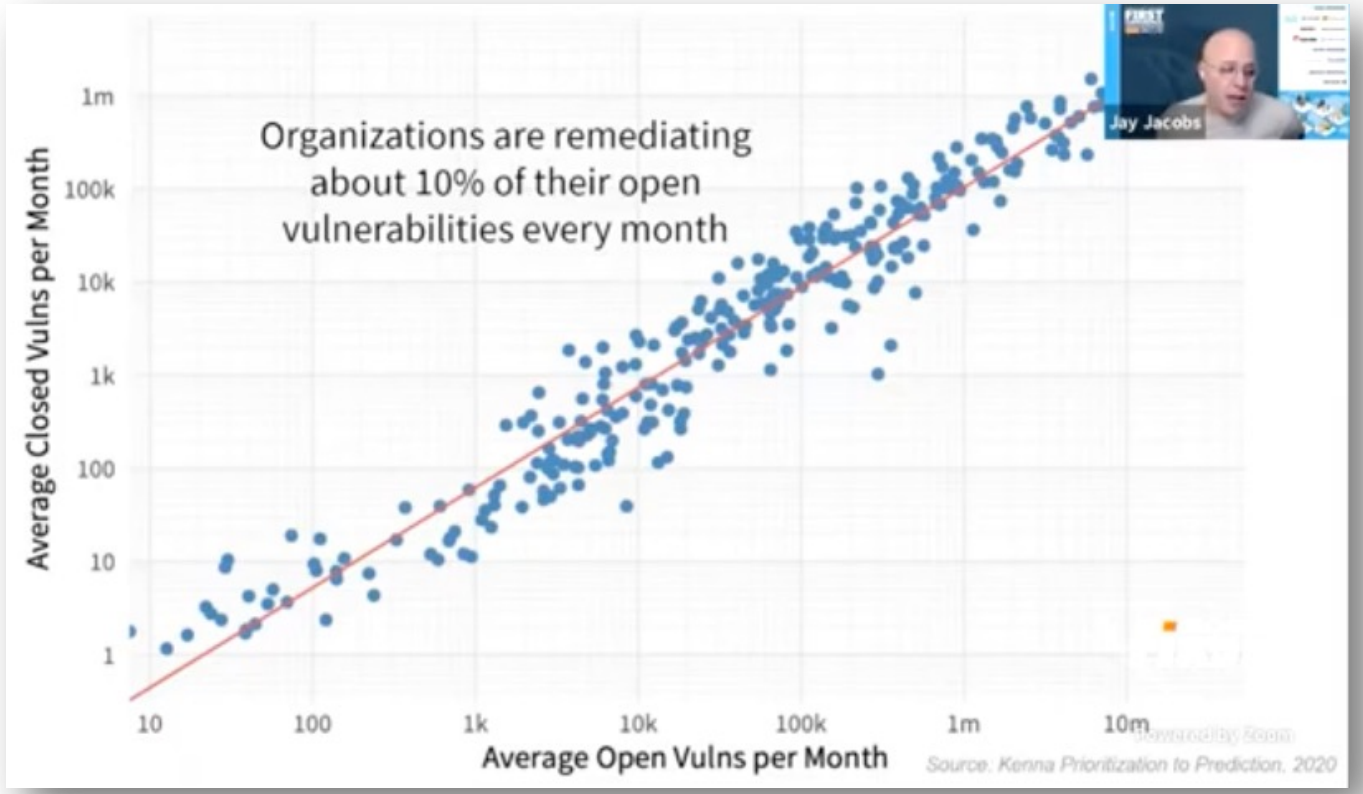


Category	Top p% vulns.	$L(p)$% of attacks
WINDOWS	20%	99.6%
	10%	96.5%
	5%	91.3%
PROD	20%	99.5%
	10%	98.3%
	5%	94.4%
BROWSER	20%	97.1%
	10%	91.3%
	5%	68.2%
PLUGIN	20%	46.9%
	10%	31%
	5%	24%

Towards Real World Cyber Risk (Panel), FIRST 2021 Conference - https://youtu.be/eyYNPLE2
http://seconomicsproject.eu/sites/default/files/seconomics/public/content-files/downloads/Comparing%20Vulnerabilities%20and%20Exploits%20using%20case%20control%20studies.pdf
https://lallodi.github.io/publications/allodi-essos-15.pdf

Uma Empresa Consegue Aplicar Todos os Patches?

- Pesquisas mostram que as empresas conseguem aplicar, em média, apenas 10% das correções para vulnerabilidades presentes em suas infraestruturas em um dado mês
- Fato: é impossível corrigir tudo
- Questões chave:
  - O que corrigir primeiro?
  - Qual métrica usar?
  - O fornecedor de segurança sabe mesmo o que é **prioritário** para o **seu ambiente**?
  - **O que tem mais chances de ser explorado?**



Towards Real World Cyber Risk (Panel), FIRST 2021 Conference - https://youtu.be/eyYNPLE2

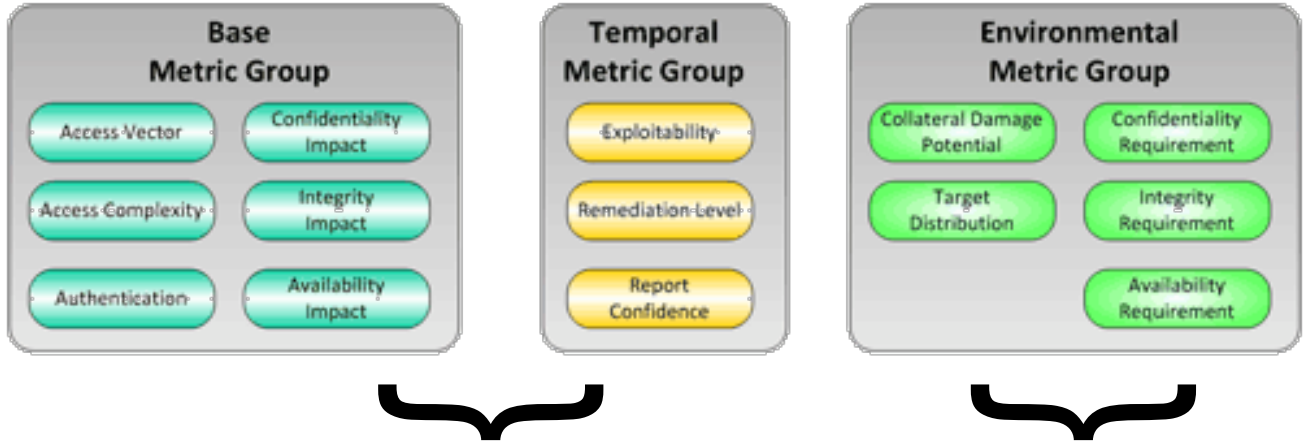
Definindo Prioridades:
CVSS - *Common Vulnerability Scoring System*

Pontos fortes

- classifica de acordo com impacto na triade CIA
- prioriza vulnerabilidades remotas e que já possuam exploits públicos
- permite personalizar para cada organização

Pontos fracos

- muitas vulnerabilidades podem ser >= 9
- não é possível saber qual tem mais probabilidade:
  - de vir a ter um exploit
  - de ser explorada por APT (Advanced Persistent Threats)



Pode ser definido por um agente externo, sem conhecer detalhes da sua infraestrutura

- Fabricante
- Empresa fornecedora de soluções de segurança

Só pode ser definido por quem conhece

- Infraestrutura interna
- Parque instalado
- Resultado da análise de risco

Definindo Prioridades:
EPSS - *Exploit Prediction Scoring System*

O que é

- Método preditivo da probabilidade de exploração de uma vulnerabilidade
- Na fórumla:

  `Risk = Threat X Vulnerability X Impact`

  EPSS define o valor de **`Threat`**
- Dados diários disponíveis
  - Top CVEs das últimas 48h, 30d e 90d
  - CVEs aumentando de prioridade

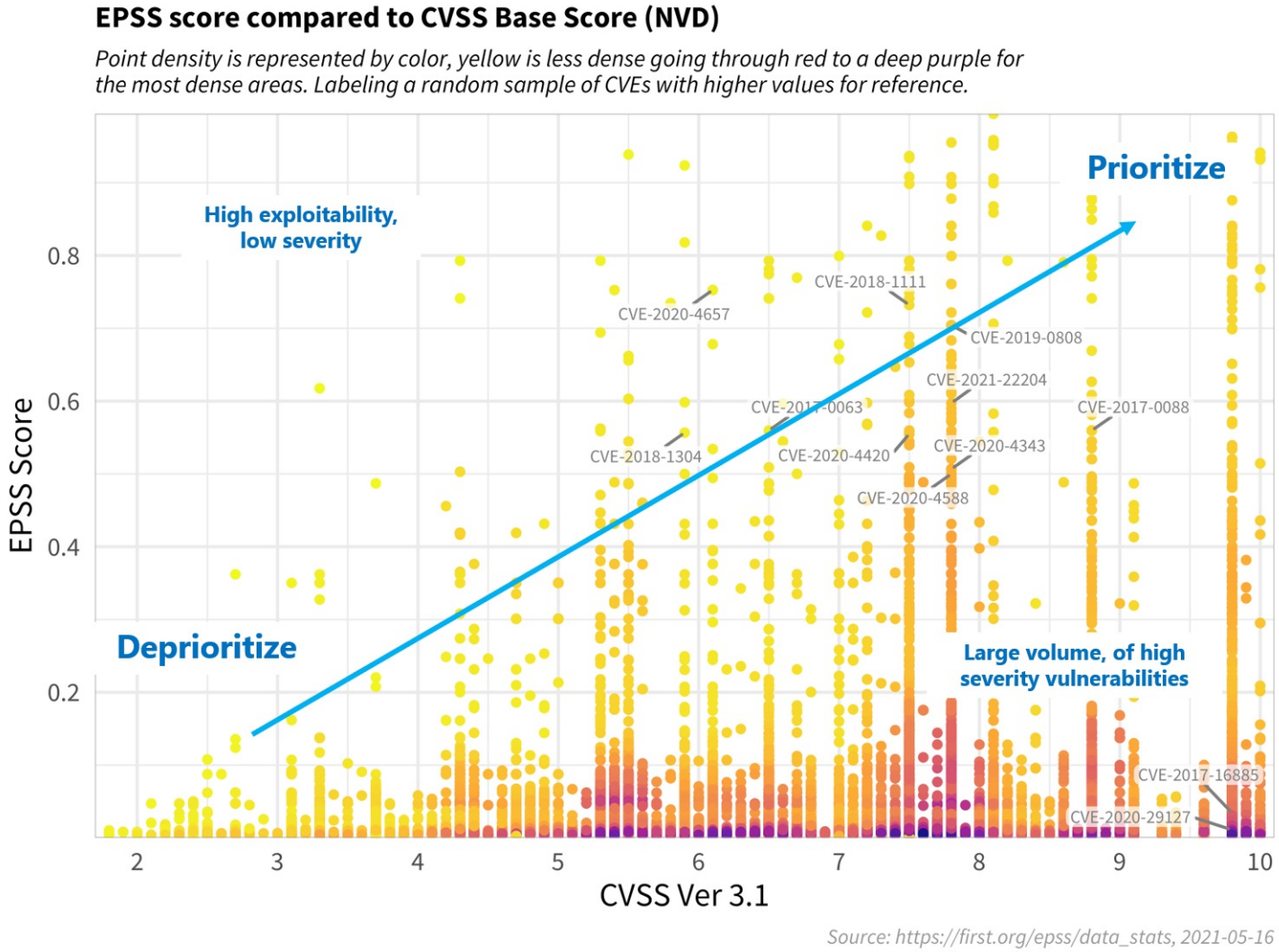
Informações

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

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

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

Towards Real World Cyber Risk (Panel)
FIRST 2021 Conference
https://youtu.be/eyYNPLE2



Por um Ecossistema mais Saudável:
Programa por uma Internet mais Segura

PROGRAMA INTERNET +SEGURA

https://bcp.nic.br/i+seg

Atuando em Conscientização desde 2000: **Portal InternetSegura.br**

Cartilha de Segurança para Internet:
Novo Design e Lançamento do Material com a ANPD

Download

Fascículo Proteção de Dados:

PDF

Slides para a divulgação das boas práticas:

PDF

PDF com notas, para impressão

LibreOffice | PowerPoint

https://cartilha.cert.br/

Obrigada

cristine@cert.br

notificações para: cert@cert.br

@certbr

https://cert.br/

nic.br cgi.br

www.nic.br | www.cgi.br