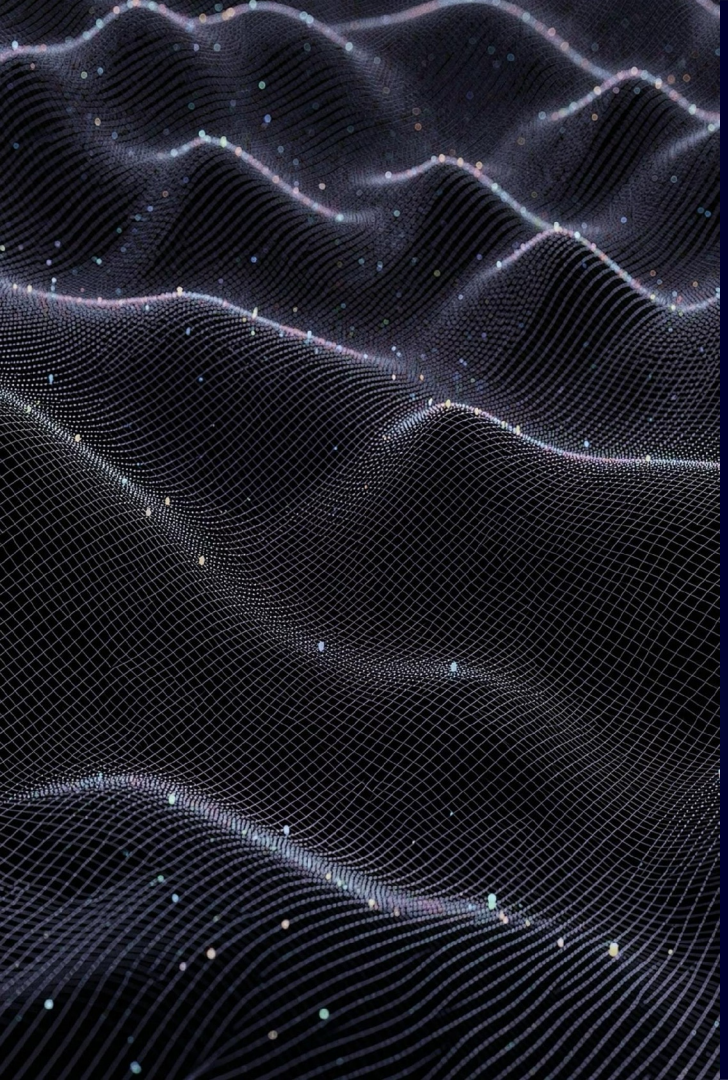


Da severidade ao risco real: a evolução da priorização de vulnerabilidades no TRE-TO

Valdenir Júnior · Fernando Ebrahim · Ulisses Jardim

TRE-TO | 14º Fórum Brasileiro de CSIRTs | São Paulo, 2026

TLP:CLEAR

Quem somos

Valdenir Júnior

Secretário de Tecnologia da Informação do TRE-TO

Fernando Ebrahim

Professor do IFTO e gestor de infraestrutura no TRE-TO

Ulisses Jardim

Assessor de Segurança Cibernética do TRE-TO

Disclaimer: Esta apresentação constitui um estudo de caso prático no TRE-TO. As opiniões e metodologias expressas são de responsabilidade dos autores e não refletem necessariamente o posicionamento oficial da Justiça Eleitoral.

TLP:CLEAR

Estruturação da segurança cibernética no TRE-TO

1
2020

ETIR formada com 9 servidores.

2
2021

1 servidor exclusivamente dedicado à segurança cibernética.

3
2022

Uso mais estruturado da ferramenta de gestão de vulnerabilidades.

4
2023

Unidade específica com equipe de 3 pessoas.

Apoio à área: ETIR · Times de TI (Infra e Desenvolvimento) · Alta Direção (STI, DG e Presidência)

TLP:CLEAR

Porque a nossa forma de trabalhar era ineficiente?

5–20%

Correções mensais

Organizações costumam corrigir apenas 5% a 20% das vulnerabilidades conhecidas por mês (Cyentia Institute)

2–7%

Exploradas in the wild

Só um subconjunto pequeno, de 2% a 7%, tende a ser explorado in the wild (Secpod)

1,4%

Exploração observada

Apenas 1,4% das vulnerabilidades publicadas tiveram exploração observada no mundo real. (Dumitras, USENIX Security 2015)

O diagnóstico central

O problema não era falta de trabalho: era decidir melhor o que tratar primeiro.

TLP:CLEAR

Nosso parceiro no processo: CERT.br

Aproximação inicial após palestra no STF

Capacitação estruturada

Participação em cursos de fundamentos e avançado de gestão de incidentes cibernéticos. **8 servidores** capacitados ao total.

Novo conceito

Contato com o conceito de priorização de vulnerabilidades baseada em dados.

A nossa ferramenta de gestão de vulnerabilidades teria suporte a esse modelo de priorização orientado a dados?

TLP:CLEAR

Da severidade ao risco real

Antes

- Severidade (CVSS)
- Criticidade do ativo
- Score de risco da plataforma

Depois

- Exploração conhecida (KEV)
- Probabilidade de exploração (EPSS)

Pergunta nova: "O que tem maior chance de ser usado contra nós agora ou em breve?"

TLP:CLEAR

KEV e EPSS

KEV

Known Exploited Vulnerabilities

- Catálogo da CISA com Vulnerabilidades com evidência confiável de exploração ativa
- Que já possuem correção/patch

EPSS

Exploit Prediction Scoring System

- Estimativa probabilística de exploração nos próximos 30 dias
- Modelo orientado a dados
- Machine Learning: Ground truth, exploit publicado, mídias sociais, listas públicas, dentre outros..

Uso complementar: primeiro KEV (exploração confirmada), depois EPSS (probabilidade de exploração).

TLP:CLEAR

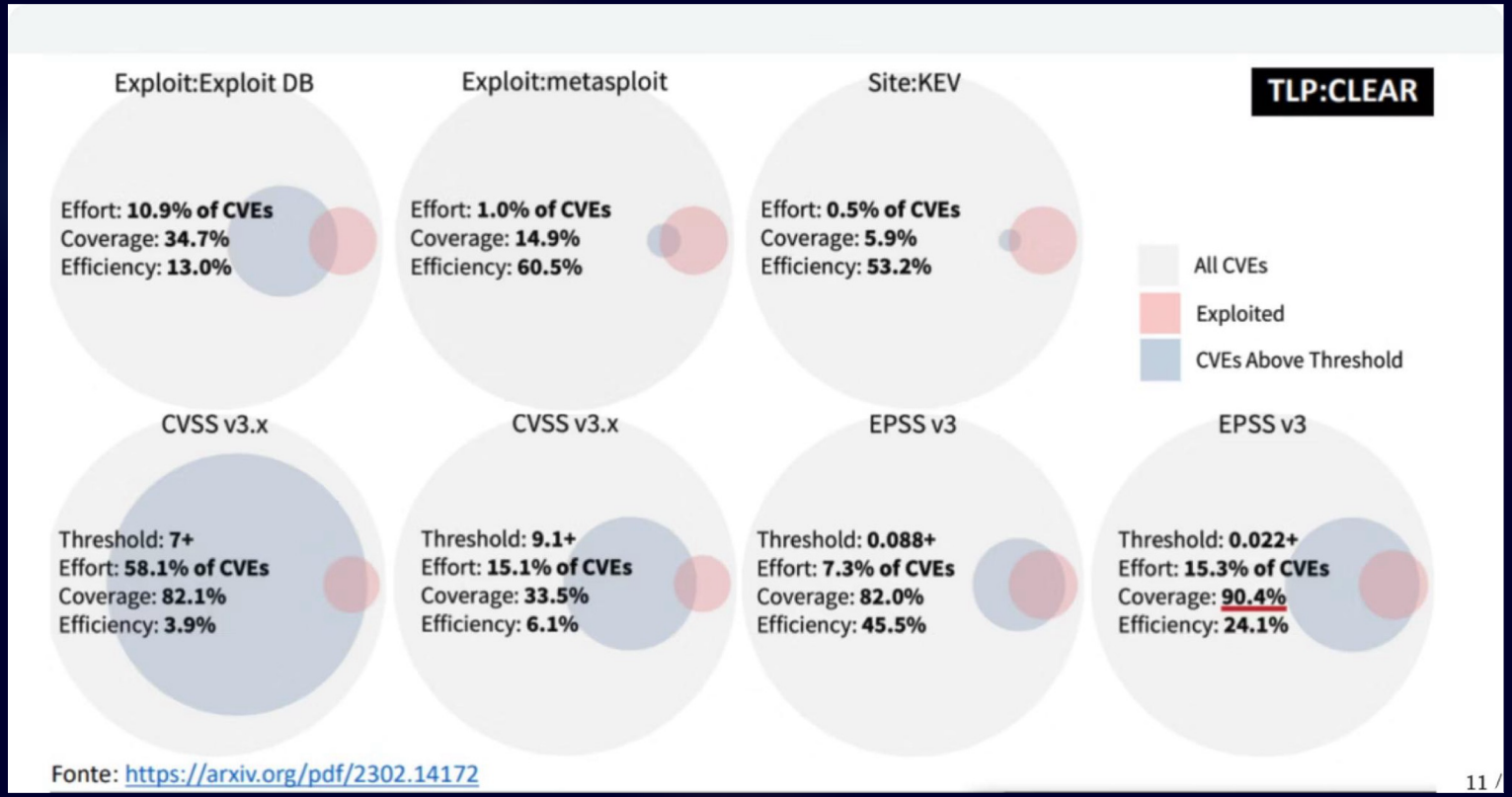
Por que EPSS 8,8%?

A nota de corte veio do treinamento do CERT.br, baseada no ponto de melhor eficiência com boa cobertura das vulnerabilidades com maior probabilidade de exploração.

Modelo	Esforço	Cobertura	Eficiência
CVSS 7+	58,1%	82,1%	3,9%
EPSS ⩾ 0,088	**7,3%**	**82,0%**	**45,5%**
EPSS ⩾ 0,022	15,3%	90,4%	24,1%

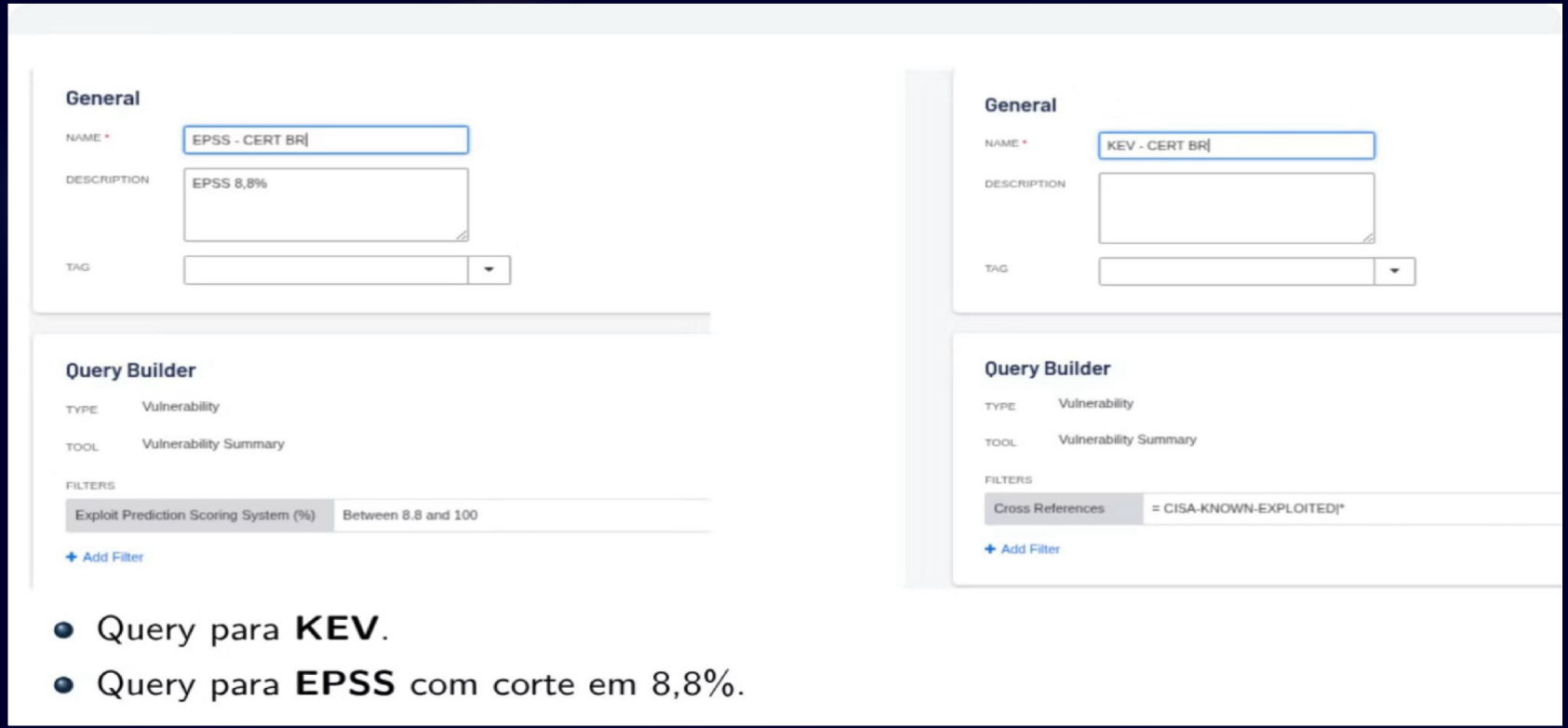
Com EPSS ⩾ 0,088, o TRE-TO alcança a mesma cobertura do CVSS 7+ (≈82%) com apenas **7,3% do esforço** — resultando em eficiência **11,7× maior**. O threshold de 8,8% representa o ponto ótimo entre cobertura e custo operacional.

Enhancing Vulnerability Prioritization: Data-Driven Exploit Predictions with Community-Driven Insights



TLP:CLEAR

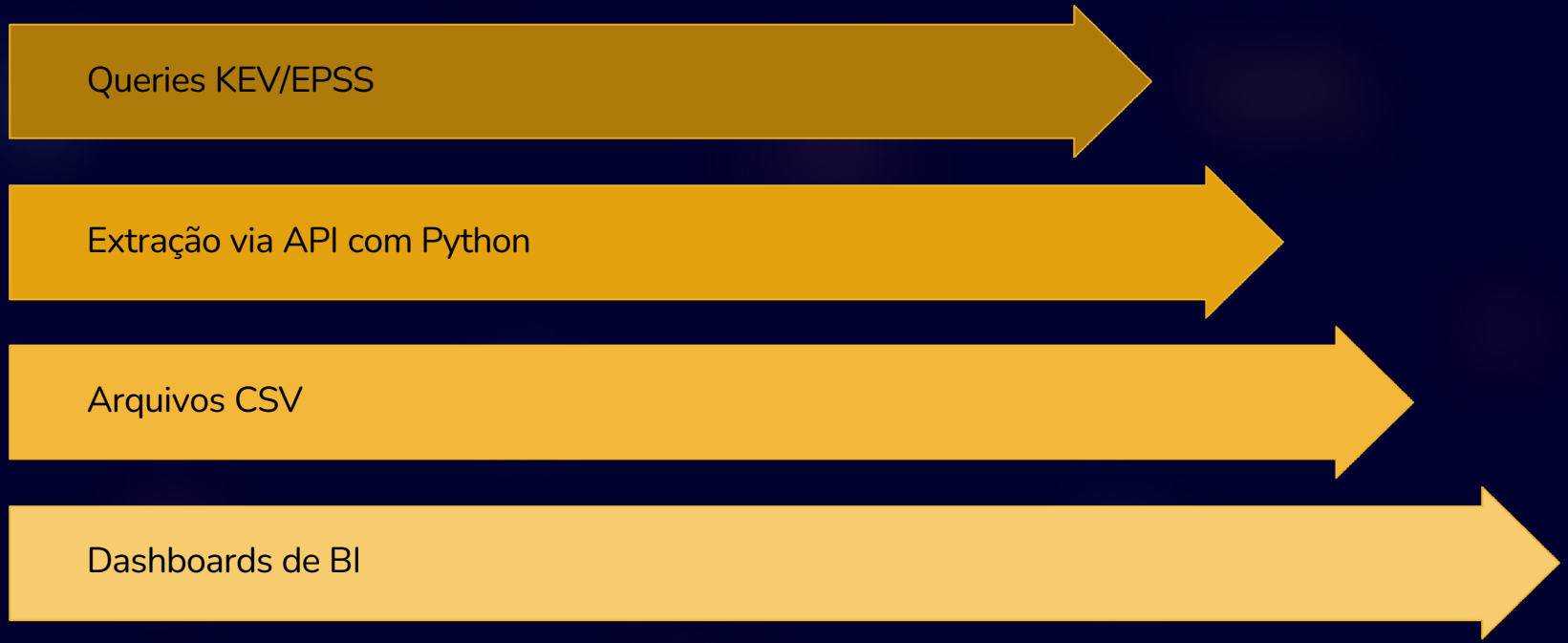
Vamos à pratica: Implementação na ferramenta



- Query para **KEV**.
- Query para **EPSS** com corte em 8,8%.

TLP:CLEAR

Automação e integração com BI



TLP:CLEAR

Ganhos com a nova metodologia

Visibilidade

Hoje sabemos exatamente quais ativos possuem vulnerabilidades KEV e EPSS > 8,8%, com rastreabilidade e histórico de evolução.

Patching

Os dashboards revelam gargalos, atrasos e obstáculos na estratégia de atualização, permitindo intervenção direcionada.

Mitigação

Conseguimos adotar medidas compensatórias quando não é possível corrigir de imediato — especialmente relevante para software legado.

Priorização

O esforço da equipe passou a ser aplicado onde o risco é mais concreto.

Gestão de ativos

Máquinas muito expostas passaram a ser questionadas quanto a dono e utilidade.

TLP:CLEAR

Lições aprendidas

1

Ferramenta sozinha não resolve o problema de priorização

2

Invista em capacitação

3

KEV e EPSS otimizam os esforços. Mais ainda para pequenas equipes.

TLP:CLEAR

Referências

Allodi et al.

Risk-based vulnerability prioritization: evidence from exploitation in the wild. Oxford Cybersecurity. Base empírica para os dados de exploração observada (1,4%) e eficiência comparativa entre modelos de priorização.

CERT.br

Entendendo CVSS, EPSS, SSVC, CVD e VDP. Palestra no fórum de CSIRTS 2024.

Cyentia Institute

Patching Fast and Slow. Estudo de referência sobre a capacidade real de remediação das organizações — base para os dados de 5% a 20% de correções mensais.

TLP:CLEAR

Obrigado

Perguntas?

Valdenir Júnior

Secretário de Tecnologia da Informação — TRE-TO

Fernando Ebrahim

Professor IFTO · Gestor de Infraestrutura — TRE-TO

Ulisses Jardim

Assessor de Segurança Cibernética — TRE-TO