csurface

WHITEPAPER · THREAT INTELLIGENCE

Por que CVSS te faz priorizar o errado

Threat Intelligence e priorização dinâmica: como acertar a fila de remediação combinando severidade técnica, exploitabilidade real (índice de probabilidade de exploração e catálogo de exploração ativa) e criticidade do ativo.

CAPACIDADE	PÚBLICO	EDIÇÃO
Threat Intelligence	**CISO · Vuln. Manager · SOC**	**2026**

LEITURA	CLASSIFICAÇÃO	FONTE
9 páginas	**Público**	**Plataforma CSURFACE**

SUMÁRIO EXECUTIVO

A fila certa de remediação não é estática

A tese deste whitepaper, em uma página — o que executivos precisam saber antes do detalhe técnico.

CVES POR TRÁS DOS BREACHES

5%

das CVEs respondem por 20% das violações reais

JANELA DE WEAPONIZAÇÃO

24h

28% das vulnerabilidades exploradas são armadas em 24 horas

REMEDIAÇÃO MENSAL TÍPICA

15%

do backlog é corrigido por mês — insuficiente para conter o ritmo de entrada

A maioria dos programas de Vulnerability Management prioriza pelo CVSS. É uma escolha intuitiva e tecnicamente insuficiente. O CVSS quantifica a **severidade técnica teórica** de uma vulnerabilidade — o impacto que ela produziria *se* fosse explorada. Ele não indica se ela **está sendo explorada no presente**, tampouco pondera a criticidade do ativo em que reside.

O resultado é uma fila sistematicamente desalinhada com o risco real. Equipes alocam capacidade escassa em vulnerabilidades de CVSS elevado e baixa exploitabilidade, enquanto vulnerabilidades de severidade média — porém ativamente exploradas em campanhas em curso — permanecem em aberto. Apenas **5% das CVEs respondem por 20% das violações** (Verizon DBIR 2024); priorizar pelo CVSS é, na prática, ignorar essa concentração de risco.

Este whitepaper apresenta a abordagem da CSURFACE: **priorização dinâmica em três eixos** — severidade técnica, exploitabilidade real (via índice de probabilidade de exploração e catálogo de exploração ativa) e criticidade do ativo —, reavaliada continuamente conforme o cenário de ameaças evolui. Uma CVE de 7.5 pode tornar-se prioridade máxima no dia seguinte ao ingresso no catálogo de exploração ativa. A fila precisa refletir essa dinâmica.

A tese. Priorização eficaz é um problema de inteligência de ameaças. A fila adequada constitui um ranking dinâmico, reordenado cada vez que um exploit se torna disponível, uma família de ransomware incorpora a vulnerabilidade ou a CISA confirma exploração ativa. Listas fixadas no momento do *disclosure* ficam desalinhadas em dias.

O que este whitepaper cobre

- Por que o volume de CVEs cresceu — e por que o CVSS não escala com ele.
- As três razões pelas quais o CVSS, sozinho, leva à fila errada.
- O modelo de priorização em três eixos da CSURFACE.
- Como o feed de inteligência se mantém dinâmico e um caso de uso real.

Sumário Executivo
O Cenário
Por que CVSS Falha
Priorização em 3 Eixos
O Feed Dinâmico
Aplicação e Resultados
Próximos Passos

O CENÁRIO · PARTE 01

O crescimento de vulnerabilidades — e a fila que não recua

Volume de publicações, capacidade de remediação e a razão pela qual a pergunta central deixou de ser quantitativa.

Whitepaper 2026
CSURFACE

~30 mil
CVEs publicadas em 2024 — 15% a mais que em 2023; a estimativa para 2025 chega a 48 mil

~15 mil
vulnerabilidades por ano no inventário de uma organização de porte médio

15% / mês
taxa típica de remediação do backlog — abaixo do ritmo de entrada de novas CVEs

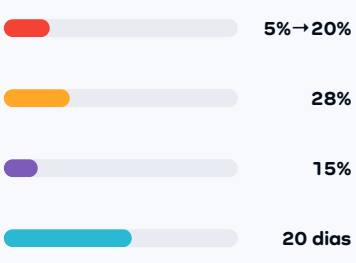
O volume cresceu mais rápido que a capacidade

O número de CVEs publicadas todo ano deixou de ser um detalhe administrativo e tornou-se um problema de capacidade. Foram cerca de **30 mil CVEs em 2024** — 15% a mais que em 2023 — e a estimativa para 2025 chega a **48 mil**, um salto da ordem de 60%.

Uma organização de porte médio precisa lidar com algo próximo de **15 mil vulnerabilidades por ano** no seu inventário. A taxa típica de remediação, porém, fica em torno de **15% do backlog por mês** (Cyentia). O diferencial entre entrada e saída é negativo de forma estrutural: o backlog cresce consistentemente.

Diante dessa assimetria, a pergunta central deixa de ser *"quantas vulnerabilidades temos?"* e passa a ser: **"estamos corrigindo as que representam risco real?"**

Estatísticas-chave



Fontes: Verizon DBIR 2024, CISA 2024, Cyentia, Snyk — relatórios públicos.

O custo de errar a fila. O custo médio de uma violação de dados no Brasil chegou a **R$ 7,19 milhões** em 2025 (IBM Cost of a Data Breach 2025). Cada vulnerabilidade ativamente explorada postergada na fila representa exposição direta pelo período do atraso. Priorizar com precisão representa a distinção entre um programa de remediação que efetivamente reduz risco e um que absorve capacidade sem direcionar esforço ao ponto de maior probabilidade de impacto.

Por que isso importa. A capacidade de remediação é finita e não vai acompanhar o volume de CVEs. A única alavanca real é a ordem da fila: corrigir primeiro o que tem maior probabilidade de ser explorado, no ativo que mais importa.

Sumário Executivo
O Cenário
Por que CVSS Falha
Priorização em 3 Eixos
O Feed Dinâmico
Aplicação e Resultados
Próximos Passos

POR QUE CVSS FALHA · PARTE 02

O CVSS mede impacto teórico — não risco real

As três razões pelas quais priorizar exclusivamente pela pontuação CVSS leva ao alvo errado.

Whitepaper 2026
CSURFACE

PELO CVSS · CORRIGE PRIMEIRO

9.8

CVSS "crítica" — porém sem exploit público, ausente de kits de ransomware e exigindo condições raríssimas de ambiente para funcionar.

→

PELA REALIDADE · É A URGÊNCIA

7.5

CVSS "alta" — com exploit público publicado, no catálogo de exploração ativa e ativamente usada por famílias de ransomware em campanhas reais.

Um número, três pontos cegos

O CVSS quantifica o impacto teórico *caso* a vulnerabilidade seja explorada. Ele não responde à pergunta operacional — ela **está sendo explorada agora?**. O contraste acima resume o problema: pelo CVSS, a equipe corrige a 9.8 primeiro; pela realidade do risco, a 7.5 é a urgência. A pontuação técnica, sozinha, conduz à decisão inversa da correta.

O motivo é estrutural. As três razões a seguir explicam por que priorizar exclusivamente pela pontuação CVSS leva ao alvo errado — e por que nenhuma delas se resolve calibrando melhor o próprio CVSS.

Razão 01 · CVSS mede severidade, não exploitabilidade. A pontuação responde "quão grave seria", não "isto está sendo explorado". É o eixo que o exemplo acima expõe.

Razão 02 · CVSS ignora o contexto do ativo. Uma vulnerabilidade 9.8 em um servidor de produção com dados de cartão é catastrófica. A mesma 9.8 em uma máquina de teste isolada, sem dados, é praticamente irrelevante. O CVSS atribui a ambas o mesmo número — e qualquer fila construída só sobre ele trata casos incomparáveis como iguais.

O QUE A CSURFACE OBSERVA · DADOS PRÓPRIOS DA PLATAFORMA

5,7%
das 2.361 vulnerabilidades analisadas têm exploit público — e só 1,8% estão no catálogo de exploração ativa

19%
de um feed de ameaças de CVSS médio 9,0 exigem ação imediata na categorização SSVC

~5 dias
é o tempo médio até surgir um exploit público após a divulgação de uma falha

Razão 03. CVSS é estático; o risco muda continuamente

A pontuação é atribuída no *disclosure* e raramente revista. O cenário de ameaças, porém, evolui em dias. Veja a trajetória típica de uma mesma CVE:

1. **Dia 0 — disclosure.** A CVE recebe CVSS 7.5. A fila a coloca como prioridade média.
2. **Dia 3 — prova de conceito.** Um exploit funcional é publicado em repositório público. A barreira para o ataque despenca.
3. **Dia 7 — adoção criminosa.** Famílias de ransomware passam a incorporar a vulnerabilidade às suas campanhas.
4. **Dia 14 — confirmação oficial.** A CVE entra no catálogo de exploração ativa, atestando exploração ativa em ataques reais.

O CVSS continua 7.5 do dia 0 ao dia 14. O risco real, nesse intervalo, subiu várias vezes — e a fila estática nunca registrou a mudança.

Sumário Executivo
O Cenário
Por que CVSS Falha
Priorização em 3 Eixos
O Feed Dinâmico
Aplicação e Resultados
Próximos Passos

A ABORDAGEM CSURFACE · PARTE 03

Priorização dinâmica em três eixos

Severidade técnica, exploitabilidade real e criticidade do ativo — combinados em um único score vivo.

Whitepaper 2026
CSURFACE

OS TRÊS EIXOS DA PRIORIZAÇÃO DINÂMICA

1 **Severidade técnica**
O CVSS como *baseline* de impacto, em escala de 0 a 10. Eixo estável — raramente muda após o disclosure.

×

2 **Exploitabilidade real**
A probabilidade concreta de exploração, de 0 a 1 — somando índice de probabilidade de exploração, catálogo de exploração ativa, inteligência ativa e ransomware.

×

3 **Criticidade do ativo**
Um multiplicador de 0,5 a 2,0: a mesma vulnerabilidade não pesa igual em todo lugar.

O que compõe a exploitabilidade real

O Eixo 02 é o que o CVSS não cobre. Ele resulta da soma de quatro evidências independentes, cada uma com a sua própria cadência de atualização:

CRÍTICO **Probabilidade de exploração**
Estima a probabilidade estatística de exploração nos próximos 30 dias, atualizada diariamente.

CRÍTICO **Catálogo de exploração ativa**
Catálogo de vulnerabilidades comprovadamente exploradas em ataques reais. Constar nele significa prioridade automática.

ATENÇÃO **Inteligência ativa**
Monitoramento de kits de exploração, fóruns de comércio criminoso e repositórios públicos de provas de conceito.

ATENÇÃO **Indicadores de ransomware**
Associação a famílias ativas — sinal de adoção operacional da vulnerabilidade por atacantes.

O score final

Os três eixos se combinam em um único índice de prioridade:

prioridade = severidade × exploitabilidade × criticidade

O produto importa: uma severidade alta multiplicada por uma exploitabilidade quase nula recua na fila; uma severidade média multiplicada por exploitabilidade alta em um ativo crítico sobe ao topo.

Como o ativo é classificado. A CSURFACE avalia sensibilidade de dados (pessoais e sensíveis sob LGPD, dados de cartão sob PCI), exposição (público, intranet ou segregado), criticidade de negócio e posição na cadeia — de frontend voltado ao cliente a backoffice.

Por que multiplicar, não somar. Um produto faz qualquer eixo próximo de zero derrubar a prioridade inteira — uma severidade 9.8 com exploitabilidade quase nula recua na fila. A soma jamais produziria esse efeito: ela sempre manteria o número alto no topo.

Sumário Executivo
O Cenário
Por que CVSS Falha
Priorização em 3 Eixos
O Feed Dinâmico
Aplicação e Resultados
Próximos Passos

A ABORDAGEM CSURFACE · PARTE 03

Um feed de inteligência continuamente atualizado

As fontes integradas e o ciclo fechado que reordena a fila de prioridades sem dependência de intervenção manual.

Whitepaper 2026
CSURFACE

O CICLO FECHADO DE REAVALIAÇÃO — SEM INTERVENÇÃO MANUAL

1 Reavaliação automática
O score de prioridade é recalculado sem nenhum acionamento manual quando a CVE muda de status.

→

2 Notificação dirigida
Mudanças materiais — como a entrada de uma CVE no catálogo de exploração ativa — geram alerta imediato.

→

3 Ticket sincronizado
O chamado em Jira ou ServiceNow é atualizado, e o SLA acompanha a nova prioridade.

→

4 Painel executivo atualizado
O painel de gestão reflete a fila reordenada em tempo real, dispensando o ciclo periódico de relatório.

Fontes integradas

A priorização só é dinâmica porque o feed de inteligência também é. A CSURFACE integra e cruza, de forma contínua:

CRÍTICO **Probabilidade de exploração**
Feed diário de probabilidade de exploração.

CRÍTICO **Catálogo de exploração ativa**
Catálogo de exploração ativa, atualizado em horas.

NVD
Dados-base das CVEs e seus metadados oficiais.

Avisos de fabricantes
Boletins de segurança dos fornecedores afetados.

ATENÇÃO **Provas de conceito públicas**
Incluindo Exploit-DB e repositórios abertos.

ATENÇÃO **Monitoramento criminoso**
Discussão e comércio de exploits em fóruns fechados.

ATENÇÃO **Sinais de honeypot**
Quando uma vulnerabilidade começa a ser varrida em larga escala.

Por que o feed precisa ser contínuo

Uma fila estática só seria suficiente se o cenário de ameaças também o fosse. Um exploit pode surgir três dias após o disclosure; a CISA pode confirmar exploração ativa poucos dias depois. Cada uma dessas mudanças altera a prioridade real de uma CVE — e, se o feed não as registra no mesmo dia, a fila opera sobre dados desatualizados, desconectada do risco vigente.

Por isso a CSURFACE trata a inteligência como um fluxo contínuo. Cada fonte ao lado tem cadência própria, e o ciclo fechado descrito acima garante que toda mudança material alcance a fila — e a equipe responsável — sem depender da percepção individual de um analista.

Ritmo de cada eixo. A severidade técnica é praticamente estática. A exploitabilidade é reavaliada diariamente — o índice de probabilidade de exploração roda todo dia, o catálogo de exploração ativa em horas, a inteligência ativa em tempo real. A criticidade do ativo é revista mensalmente ou a cada mudança de configuração.

Sumário Executivo
O Cenário
Por que CVSS Falha
Priorização em 3 Eixos
O Feed Dinâmico
Aplicação e Resultados
Próximos Passos

APLICAÇÃO E RESULTADOS · PARTE 04

A mesma equipe, uma fila diferente

Um caso de uso representativo: como a priorização dinâmica reordenou o topo da fila sem aumentar a capacidade.

PRIORIZAÇÃO POR CVSS

3

incidentes materiais em 12 meses — todos em CVEs de CVSS 7.x, porém presentes no catálogo de exploração ativa.

→

PRIORIZAÇÃO DINÂMICA CSURFACE

0

incidentes materiais nos 6 meses seguintes, com a mesma equipe e a mesma capacidade de remediação.

Caso de uso · banco de médio porte

Uma instituição financeira de médio porte operava com **4.200 ativos** e cerca de **8.700 CVEs ativas**. A equipe — quatro responsáveis por correção e dois desenvolvedores — tinha capacidade para cerca de 80 correções por mês, contra um backlog que crescia 50 por mês. A fila priorizava as 200 vulnerabilidades de CVSS 9.0 ou mais.

Os três incidentes registrados em doze meses ocorreram, todos, em vulnerabilidades de CVSS na faixa 7.x — abaixo do corte de "crítica" — mas presentes no catálogo de exploração ativa. A fila por CVSS as havia deixado de fora.

Com a priorização dinâmica, o topo da fila foi reordenado sem alterar a capacidade da equipe.

Como o topo da fila mudou

47 vulnerabilidades saíram da lista de críticas
CVSS alto, mas probabilidade de exploração abaixo de 0,05 e sem qualquer sinal de exploração.

CRÍTICO **89 entraram no topo da fila**
CVSS médio, porém com probabilidade de exploração acima de 0,5 ou já no catálogo de exploração ativa.

ATENÇÃO **31 subiram de posição**
Exclusivamente pelo multiplicador de criticidade do ativo.

O resultado. A capacidade de remediação passou a ser direcionada para onde o risco efetivamente estava concentrado. Nos seis meses seguintes, os incidentes materiais caíram de três para zero — sem ampliação de equipe ou orçamento adicional.

A capacidade não mudou — a alocação sim. A equipe manteve o ritmo de cerca de 80 correções por mês. O que se alterou foi a composição dessas correções: o esforço deixou de ser absorvido por vulnerabilidades de CVSS elevado sem exploração ativa e passou a cobrir as que apresentavam exploração real nos ativos de maior criticidade.

Sumário Executivo
O Cenário
Por que CVSS Falha
Priorização em 3 Eixos
O Feed Dinâmico
Aplicação e Resultados
Próximos Passos

APLICAÇÃO E RESULTADOS · PARTE 04

Métricas de mudança e integração na plataforma

Variações nos indicadores do programa e articulação da priorização dinâmica com as demais capacidades da plataforma.

Métricas de mudança · banco de médio porte

INDICADOR	ANTES · PRIORIZAÇÃO POR CVSS	DEPOIS · PRIORIZAÇÃO DINÂMICA	VARIAÇÃO
MTTR de vulnerabilidades críticas exploradas	87 dias	18 dias	-79%
Correções aplicadas em CVEs com exploração real	45%	92%	+47 pp
Saldo mensal do backlog	+50	-12	revertido
Falsos positivos na classificação "crítica"	30%	8%	-22 pp
Incidentes materiais por ano	3	0 (em 6 meses)	-100%

Indicadores observados no caso de uso descrito na página anterior. Resultados variam conforme o tamanho do inventário, a capacidade de remediação e a maturidade do programa de cada organização.

-79%
no MTTR das vulnerabilidades críticas exploradas — de 87 para 18 dias

backlog
saldo mensal revertido: de +50 vulnerabilidades por mês para -12

3 → 0
incidentes materiais — de três em doze meses a zero nos seis meses seguintes

Integração com as demais capacidades

A Threat Intelligence não opera de forma isolada. Na plataforma unificada da CSURFACE, ela consome as demais capacidades e retroalimenta cada uma delas:

Descoberta contínua
Cada novo ativo da superfície externa entra automaticamente no escopo da priorização.

Validação de exploitabilidade
Confirma se a exploração é viável no contexto real do ambiente, refinando o eixo de exploitabilidade.

CRÍTICO **Monitoramento de credenciais vazadas**
Credenciais comprometidas somadas a uma vulnerabilidade crítica elevam a prioridade ao máximo.

Da fila ao valor financeiro. A prioridade calculada alimenta a calculadora de risco da CSURFACE, que estima a perda anual esperada por setor. Quanto maior a prioridade de uma vulnerabilidade, maior o custo de mantê-la em aberto — uma leitura que traduz a fila técnica em linguagem de negócio acessível ao conselho e ao comitê de auditoria.

Indicadores-chave do programa

- MTTR das vulnerabilidades efetivamente exploradas — não da média geral do backlog.
- Percentual do esforço de remediação aplicado a CVEs com exploração confirmada.
- Saldo líquido mensal do backlog: tendência de redução ou crescimento.

Sumário Executivo
O Cenário
Por que CVSS Falha
Priorização em 3 Eixos
O Feed Dinâmico
Aplicação e Resultados
Próximos Passos

PRÓXIMOS PASSOS

A fila certa começa com inteligência de ameaças

A Threat Intelligence com priorização dinâmica é uma das capacidades da plataforma CSURFACE — uma plataforma de Continuous Exposure Management. Em arquitetura unificada, reúne descoberta contínua da superfície externa com Machine Learning, análise da cadeia digital de fornecedores, validação de exploitabilidade, inteligência de ameaças com priorização dinâmica e monitoramento de credenciais vazadas. Opera integralmente de forma externa — sem agente e sem instalação —, com integrações opcionais de nuvem, WAF e CIEM para organizações que demandam visibilidade aprofundada de ambientes internos.

Avalie como sua fila se reordenaria

Em uma demonstração de 30 minutos, apresentamos como a lista de prioridades atual se reorganizaria com a priorização dinâmica em três eixos.

Calculadora de risco financeiro

Estime a perda anual esperada por setor e quantifique o custo de manutenção de cada vulnerabilidade em aberto.

Whitepaper: ML Discovery

Descoberta contínua da superfície externa — a base de inventário sobre a qual toda priorização dinâmica precisa operar.

Conheça sua fila reordenada — pela exploração real, não pela pontuação teórica

Solicitar análise preliminar