CSURFACE

WHITEPAPER · CREDENTIAL LEAKAGE

94 dias: o tempo médio até descobrir que suas credenciais vazaram

Credential Leakage Monitor: por que o monitoramento contínuo de breach databases, dark web e repositórios públicos supera sistematicamente qualquer auditoria pontual — com validação ativa para eliminação de falsos positivos.

CAPACIDADE	PÚBLICO	EDIÇÃO
Credential Leakage Monitor	CISO · IAM Lead · SOC	2026

LEITURA	CLASSIFICAÇÃO	FONTE
7 páginas	Público	Plataforma CSURFACE

SUMÁRIO EXECUTIVO

A janela de reação é em horas, não em trimestres

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

BREACHES POR CREDENCIAL

30%

dos incidentes começam com uma credencial comprometida

TEMPO ATÉ A DETECÇÃO

94 dias

é a média entre o vazamento e a descoberta

DETECÇÃO COM MONITORAMENTO CONTÍNUO

< 24h

do vazamento ao alerta validado

Cerca de **30% das violações de dados começam com uma credencial comprometida** (Verizon DBIR). O problema central é que credenciais vazam sem serem percebidas. O intervalo médio entre o vazamento de uma credencial e a sua descoberta pela organização afetada é de **94 dias**.

Noventa e quatro dias representam uma janela operacional ampla para o atacante: tempo suficiente para concluir o reconhecimento, escalar privilégios, exfiltrar dados e, em muitos casos, encerrar a operação sem evidências imediatas. A credencial vazada constitui o vetor de acesso que precede o incidente, disponível meses antes de qualquer mecanismo de detecção interno ser acionado.

Este whitepaper apresenta o **Credential Leakage Monitor** da CSURFACE: monitoramento contínuo de bases de breaches públicos, dark web e repositórios públicos de código para detectar credenciais corporativas vazadas em horas — não em meses. A operação é inteiramente externa, sem agente ou instalação, e inclui validação ativa que confirma a vigência de cada credencial antes da emissão de qualquer alerta.

A tese. A defesa de credenciais não se resolve com auditorias periódicas. Credenciais vazam de forma contínua — e por isso precisam ser monitoradas de forma contínua. Reduzir a janela de descoberta de trimestres para horas é o que converte um incidente de meses em uma resposta contida no prazo de um dia útil.

O que este whitepaper cobre

- Por que credenciais vazam — e por que a detecção tradicional é lenta.
- As três fontes de vazamento que realmente importam para uma organização.
- Por que a validação ativa é o que separa um alerta útil de ruído.
- O workflow de resposta recomendado e um caso de uso representativo.

O CENÁRIO · PARTE 01

Credenciais vazam o tempo todo — a detecção, não

Como as credenciais corporativas chegam às mãos erradas e por que os controles tradicionais demoram a perceber.

OS CINCO CAMINHOS DO VAZAMENTO DE CREDENCIAL

CRÍTICO Breach de SaaS de terceiros
O colaborador reusou a senha corporativa; o serviço sofre violação e a credencial vai ao mercado.

CRÍTICO Phishing bem-sucedido
A credencial é digitada em página falsa e enviada diretamente ao atacante.

ATENÇÃO Repositórios públicos
Commit acidental de arquivo .env, chave de nuvem ou senha em arquivo de configuração.

CRÍTICO Infostealers
Malware no notebook pessoal exfiltra todas as senhas salvas no navegador.

ATENÇÃO Ação de insider
Colaborador descontente compartilha ou vende acessos a terceiros.

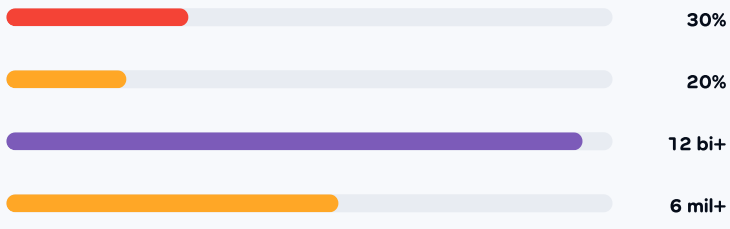
O QUE A CSURFACE OBSERVA · DADOS PRÓPRIOS DA PLATAFORMA

170
credenciais corporativas vazadas identificadas em 16 empresas analisadas pela plataforma

37%
das empresas analisadas tinham ao menos uma credencial corporativa exposta

A escala do problema

Nenhum desses cinco caminhos atravessa o perímetro que a organização controla — e nenhum aciona um alerta interno. A credencial torna-se disponível externamente, em fontes acessíveis a agentes adversários, sem que qualquer sinal interno seja gerado.



Fontes: Verizon DBIR, SpyCloud, HaveIBeenPwned, GitHub Secret Scanning Trends.

O custo de não detectar. 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), e a sanção administrativa da LGPD pode alcançar 2% do faturamento, limitada a R$ 50 milhões. Cada dia eliminado da janela de descoberta reduz a probabilidade de o vazamento evoluir para incidente — impacto que a calculadora de risco da CSURFACE traduz em perda anual esperada (ALE).

Por que a detecção é lenta. Auditorias de senha são pontuais (anuais ou semestrais); o MFA reduz risco mas não cobre contas de serviço e *legacy*; o DLP olha a saída de dados, não o retorno de uma credencial à venda em fórum; e o SIEM só detecta uso anômalo depois que o atacante já está dentro. Nenhum desses controles observa o lado de fora — exatamente onde a credencial vazada fica exposta.

AS TRÊS FONTES · PARTE 02

Onde monitorar: três fontes que importam

Breach databases, dark web e repositórios públicos — o que cada fonte revela e o que a CSURFACE faz com ela.

AS TRÊS FONTES MONITORADAS EM PARALELO

1. **Breach databases**
   Cruzamento do domínio contra bases agregadas de vazamentos públicos.
2. **Dark web**
   Monitoramento de mercados e fóruns que comercializam credenciais recentemente roubadas.
3. **Repositórios públicos**
   Varredura de novos commits em busca de secrets do ambiente do cliente.

01. Breach databases

Mais de **12 bilhões de credenciais** já foram expostas em incidentes públicos — de vazamentos históricos a coleções consolidadas. Fontes públicas como HaveIBeenPwned mantêm bases agregadas desses eventos.

O que a CSURFACE faz. Faz o cruzamento contínuo do domínio corporativo do cliente contra essas bases. Quando uma credencial vinculada ao domínio aparece em qualquer breach — mesmo de um SaaS de terceiros — a organização é notificada.

02. Dark web

Mercados, fóruns e canais de mensageria comercializam credenciais recentemente extraídas por infostealers, com atualização diária dos lotes disponíveis. Organizações de perfil relevante chegam a ter dossiês de acesso disponíveis para aquisição imediata.

O que a CSURFACE faz. Monitora comunidades conhecidas por meio de parceiros de inteligência de ameaças e identifica a venda ativa de credenciais associadas ao domínio do cliente.

03. Repositórios públicos de código

Em plataformas como GitHub, GitLab e Bitbucket, desenvolvedores publicam inadvertidamente arquivos **.env**, chaves de acesso de nuvem e senhas em arquivos de configuração — na ordem de milhares de secrets expostos por dia.

O que a CSURFACE faz. Faz a varredura contínua de novos commits públicos em busca de padrões associados ao ambiente do cliente: chaves de nuvem, tokens, hostnames internos e outros secrets.

Por que três fontes, e não uma. Cada fonte cobre um caminho distinto de vazamento: a breach database revela o reuso de senha; a dark web revela a credencial recém-roubada à venda; o repositório público revela o secret esquecido em código. Monitorar só uma delas deixa dois terços do problema invisível.

VALIDAÇÃO E WORKFLOW · PARTE 03

Validação ativa: só alertar sobre o que ainda funciona

Detectar uma credencial vazada é metade do trabalho. A outra metade é confirmar se ela ainda é uma ameaça.

Por que a validação ativa importa

Parte significativa dos vazamentos registrados é historicamente antiga: a senha já foi substituída, a chave já foi revogada, a conta já foi desativada. Emitir alertas sobre essas credenciais produz ruído operacional — e a acumulação de ruído compromete a capacidade da equipe de responder aos alertas realmente críticos.

A CSURFACE executa validação automática, segura e não destrutiva, para confirmar a vigência de cada credencial detectada. O resultado: a organização recebe notificações **exclusivamente** sobre credenciais que permanecem ativas, com redução acentuada de falsos positivos.

Como a credencial é validada, por tipo

SAML / OAuth
Uma requisição de refresh token; se aceita, a conta está ativa.

SMTP / e-mail
Uma tentativa de autenticação sem envio de mensagem.

Chaves de nuvem
Chamada somente leitura de identidade, que falha se a chave foi revogada.

Tokens de API
Consulta a um endpoint de identidade do tipo /me ou /whoami.

Validação não destrutiva. Toda verificação confirma a vigência da credencial sem alterar dados, enviar mensagens ou disparar bloqueios na conta-alvo. O objetivo é responder a uma única questão — esta credencial permanece ativa? — antes de mobilizar a equipe de segurança para investigação.

WORKFLOW DE RESPOSTA RECOMENDADO · DO ALERTA AO RISCO RECALCULADO

1. **Notificação imediata**
Alerta via Slack, e-mail ou SMS com contexto: fonte, data do vazamento, credencial parcial e resultado da validação.

→

2. **Acionamento do IdP**
Integração opcional com Okta, Microsoft Entra ID ou JumpCloud força o reset de senha e revoga sessões ativas.

→

3. **Ticket para o SOC**
Chamado automático com a evidência reunida, incluindo o histórico recente de acesso da conta, para investigação.

→

4. **Painel atualizado**
A exposição da organização é recalculada e refletida no painel, mantendo a priorização alinhada ao risco corrente.

As integrações com IdP são opcionais — a detecção e a validação operam de forma 100% externa, sem agente.

APLICAÇÃO E RESULTADOS · PARTE 04

Do alerta à resposta em horas

Um caso de uso representativo, os indicadores de resultado e o enquadramento de conformidade.

DETECÇÃO TRADICIONAL

94 dias

média entre o vazamento e a descoberta — janela suficiente para que o atacante complete o ciclo de comprometimento.

→

COM O MONITOR DA CSURFACE

< 24h

do vazamento ao alerta validado — SLA típico de notificação em menos de 4 horas.

Caso de uso · mídia, 2.500 colaboradores

Uma empresa de mídia colocou em monitoramento o domínio raiz e quatro plataformas SaaS conhecidas. Na **primeira semana**, o cruzamento com breach databases revelou o seguinte funil:

ATENÇÃO **247 credenciais expostas**
do domínio, encontradas em breaches públicos.

CRÍTICO **38 ainda válidas**
confirmadas pela validação ativa da plataforma.

CRÍTICO **12 de colaboradores atuais**
forçadas a reset imediato de senha.

ATENÇÃO **26 de ex-colaboradores**
contas órfãs em SaaS encerradas; offboarding revisado.

No **mês 2**, um novo alerta identificou uma chave de nuvem ativa publicada em repositório público. A validação confirmou a vigência da chave, que detinha permissão de leitura sobre um bucket contendo dados de clientes. A revogação foi concluída em 4 horas a partir do disclosure — antes de qualquer exploração registrada.

Indicadores de resultado

INDICADOR	BASELINE	CSURFACE
Tempo até a detecção	94 dias	**< 24 horas**
Falsos positivos	Altos	**< 5%**
Notificação após exposição	Pontual	**SLA < 4 horas**
Cobertura de fontes	Uma, se houver	**Três fontes**

Faixas observadas em monitoramentos conduzidos pela plataforma CSURFACE. O resultado varia conforme a dispersão da superfície de cada organização.

Enquadramento de conformidade. A detecção rápida sustenta a comunicação tempestiva à ANPD prevista na LGPD (Art. 46), o monitoramento de credenciais exigido pela Resolução BACEN nº 4.893, a gestão de acesso da ISO 27001 (A.9) e a identificação e autenticação do PCI DSS (Requisito 8).

PRÓXIMOS PASSOS

A defesa de credenciais começa com um único domínio

O Credential Leakage Monitor é uma das capacidades da plataforma CSURFACE — uma plataforma de Continuous Exposure Management. Em uma arquitetura integrada, 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 inteiramente de forma externa — sem agente e sem instalação —, com integrações opcionais de nuvem, WAF e CIEM disponíveis para organizações que requeiram cobertura aprofundada.

Receba a análise preliminar
Informe o domínio corporativo e receba, gratuitamente, uma avaliação das credenciais já expostas em fontes públicas associadas à sua organização.

Use a calculadora de risco
Estime a perda anual esperada (ALE) e o VaR do seu setor, com metodologia FAIR calibrada por benchmark de mercado.

Leia o próximo whitepaper
Inteligência de Ameaças e Priorização Dinâmica — como credenciais comprometidas alimentam a priorização do risco.

Veja quais credenciais já vazaram — monitoramento iniciado com o domínio raiz

Receber análise preliminar gratuita