intrus / io

WHITEPAPER · 2026

PROGRAMA CRIVO · V1.0

Antes de contratar um hacker, ele passa pelo *Crivo.*

Um framework proprietário para certificar a integridade de profissionais de segurança ofensiva antes do primeiro acesso a dados de cliente. Metodologia, fases, racional e compromissos contratuais.

DOCUMENTO TÉCNICO

INTRUS.IO / CRIVO · V1.0

CLASSIFICAÇÃO

DISTRIBUIÇÃO PÚBLICA

— § 01 · RESUMO EXECUTIVO

O vetor mais barato contra a sua empresa não é técnico.

Em segurança ofensiva, o profissional contratado recebe, por definição, o que nenhum funcionário seu recebe: acesso privilegiado ao seu ambiente, permissão explícita para tentar quebrá-lo, e permanência prolongada em sistemas que contêm seus dados mais sensíveis.

O mercado resolveu o problema da **habilidade**: há certificações (OSCP, CEH, CISSP, CRTO, GPEN) que comprovam capacidade técnica. O que o mercado não resolveu é o problema da **integridade**. Este whitepaper descreve o Crivo — o programa proprietário da intrus.io que endereça exatamente essa lacuna.

> *"Você contrata um pentester para provar que seus sistemas são invadíveis. No processo, ele passa meses dentro deles. O NDA está no papel. A tentação, não."*

87%	05	00
TAXA HISTÓRICA DE REPROVAÇÃO	PROFISSIONAIS ATIVOS PÓS-CRIVO	INCIDENTES ATRIBUÍDOS AO TIME

— § 02 · O PROBLEMA

Habilidade sobra. Caráter *quase nunca se mede.*

2.1 A ASSIMETRIA DA CONTRATAÇÃO EM CYBER

Ao contratar um desenvolvedor, um cliente contrata alguém que talvez leia o código dele. Ao contratar um pentester, contrata alguém que vai ativamente *procurar* por aquilo que é mais sensível — e documentar com precisão onde está. Os dois contratos são chamados de "serviço". Apenas um deles envolve entregar chaves de cofre a um estranho.

2.2 O QUE OS CONTROLES TÉCNICOS NÃO COBREM

DLP, CASB, UEBA e IAM são camadas maduras para conter **comportamento**. Nenhuma dessas camadas age antes de o profissional estar dentro do perímetro. No momento em que o comportamento anômalo é detectado, o dado já foi acessado, fotografado, memorizado ou copiado.

O ponto do Crivo é anterior: **separar quem deveria ter acesso de quem não deveria, antes que o acesso seja concedido.**

2.3 TRÊS CENÁRIOS DOCUMENTADOS

— **Pentester com crise financeira aguda** — operador tecnicamente excelente, mas sob pressão pessoal severa no momento do engajamento. Vetor clássico de insider threat.

— **Freelancer via marketplace** — identidade verificada apenas por perfil online, rede de origem desconhecida, sem rastreabilidade real pós-entrega.

— **Vazamento pós-engajamento** — evidências coletadas no pentest aparecem em fóruns fechados seis meses após o fim do contrato. Atribuição forense é muitas vezes impossível.

— § 03 · DEFINIÇÃO

O que é o Crivo.

Crivo [substantivo masculino, do latim *cribrum*] é o processo pelo qual todo profissional da intrus.io passa antes de receber qualquer nível de acesso a ambiente de cliente. Não é uma certificação única; é uma bateria escalonada de cinco fases, combinando análise de background, perfil psicométrico, teste de armadilha controlada, supervisão operacional e monitoramento contínuo.

PRINCÍPIO FUNDADOR

Integridade é um estado, não um atributo.

Nenhum profissional é "íntegro" em absoluto. É íntegro sob um conjunto de condições. Quando as condições mudam (divórcio, dívida, doença na família, mudança de cidade), a condição anterior deixa de ser verdadeira. Por isso o Crivo não é um carimbo de passagem — é um processo vigilante.

3.1 O QUE O CRIVO NÃO É

- **Não é uma certificação pública**. O Crivo só tem valor como compromisso interno de uma empresa que contrata e se responsabiliza integralmente pelos seus profissionais.
- **Não é um substituto de NDA**. NDA protege no tribunal, depois do dano. Crivo reduz probabilidade do dano acontecer.
- **Não é uma solução de governança automatizada**. Envolve julgamento humano em etapas críticas.

— § 04 · METODOLOGIA

As cinco fases do Crivo.

	FASE	INSTRUMENTAÇÃO
01	Background contextual Ficha criminal; análise de comportamento financeiro (dívidas ativas, padrão de gastos compatível); reputação em comunidades técnicas e fóruns fechados; referências de três últimos empregadores.	Entrevista profunda de antecedentes + verificação de registros públicos e semi-públicos.
02	Perfil psicométrico Integridade (Reid, Stanton), impulsividade (Barratt), tolerância à ambiguidade moral, propensão a racionalização (Gudjonsson).	Bateria validada + entrevista situacional estruturada com dois avaliadores independentes.
03	Teste de armadilha controlada Em ambiente isolado, o candidato encontra credenciais funcionais, dados de cartão completos com CVC, acesso a conta-teste com saldo real e arquivos rotulados como "dados de cliente". Sem orientação; sem aviso.	Três vetores de tentação plantados em momentos distintos do dia de avaliação. Toda ação é logada. Veredito: *reporta, passa; mexe sem reportar, elimina*.
04	Operação supervisionada 90 dias em projeto-espelho com carga real. Revisão par-a-par obrigatória em cada artefato. Mentor técnico + observador comportamental separados.	Sessões gravadas; métricas de disciplina operacional; avaliação 360 ao fim do período.
05	Monitoramento contínuo Auditoria aleatória de acessos e artefatos; revisão anual de status; retrabalho em fases anteriores a cada mudança relevante de contexto pessoal ou financeiro declarada.	Declaração anual assinada + trilha de auditoria disponível para clientes regulados sob demanda.

4.1 TAXA DE FILTRAGEM POR FASE

Das últimas 100 candidaturas ao programa: 22 não passaram da fase 01; 19 foram eliminados na fase 02; 31 falharam na fase 03 (maior filtro absoluto); 23 não concluíram a fase 04 com aprovação. Total de aprovados: 5.

OBSERVAÇÃO METODOLÓGICA

A reprovação não é um acidente. É o objetivo.

O desenho do Crivo pressupõe que a grande maioria dos candidatos — mesmo os tecnicamente brilhantes — falhará. Um programa que aprova 80% dos candidatos não está filtrando: está validando. O Crivo filtra.

— § 05 · COMPROMISSOS CONTRATUAIS

Seis garantias que viram cláusula de contrato.

01 Ninguém toca seu ambiente sem ter passado pelo Crivo.

Sem exceção para consultores terceirizados, estagiários ou parceiros.

02 Você recebe a lista nominal do time antes do primeiro acesso.

Nome completo, documento, papel no projeto, fase Crivo vigente. Atualizada em tempo real em caso de mudança.

03 Toda sessão é gravada e auditável.

Vídeo da tela, log de comandos, screenshots temporizadas. Retenção mínima de cinco anos para clientes em setores regulados.

04 Dados sensíveis do cliente nunca saem do ambiente do cliente.

Operamos via bastion dedicado; artefatos de relatório são anonimizados antes de transitar por qualquer rede fora do perímetro contratante.

05 O selo é revogável — inclusive pelo cliente.

A qualquer momento o cliente pode solicitar substituição nominal de qualquer profissional, sem justificativa e sem penalidade. Substituição em até 48 horas úteis.

06 Em caso de má conduta comprovada: contrato sem cobrança, e cobrimos a auditoria forense externa.

Cláusula nunca acionada desde a fundação.

— § 06 · INTEROPERABILIDADE TÉCNICA

Onde o Crivo se encaixa no seu programa de segurança.

O Crivo é ortogonal às camadas técnicas de defesa e foi desenhado para complementá-las, não substituí-las. Em termos práticos:

6.1 RELAÇÃO COM FRAMEWORKS

— **NIST SP 800-53 (PS-3, PS-6, PS-7)** — O Crivo implementa, em estrutura reforçada, os controles de screening de pessoal e acordos com fornecedores previstos no framework.

— **ISO/IEC 27001 (A.6.1.1, A.7.1.1, A.7.2)** — Screening prévio, termos contratuais de acesso e conscientização contínua têm correspondência direta com as fases 01, 02 e 05.

— **OWASP / PTES / MITRE ATT&CK** — A entrega técnica dos profissionais Crivo-certificados continua seguindo esses frameworks integralmente. Crivo não altera a metodologia de engajamento; filtra quem a executa.

6.2 INTEGRAÇÃO COM CONTROLES DO CLIENTE

— Credenciais provisionadas pelo IAM do cliente, com identidade nominal (sem contas genéricas).

— Logs de sessão entregáveis no formato de SIEM do cliente (Splunk, Elastic, Sentinel).

— Aprovação prévia de todo acesso fora do escopo originalmente contratado.

— § 07 · DILIGÊNCIA PELO CONTRATANTE

Perguntas que você deveria fazer para qualquer fornecedor de pentest.

Independentemente de o cliente contratar a intrus.io, este é um checklist mínimo para avaliação de fornecedores em engajamentos de segurança ofensiva. Sugerimos copiar e aplicar.

01 Quantas pessoas terão acesso ao meu ambiente?

Peça a lista nominal. Se o fornecedor recusar, encerre a conversa.

02 Como essas pessoas são contratadas e verificadas?

NDA não é processo. Peça a metodologia de screening por escrito.

03 Posso solicitar substituição sem justificativa?

Se a resposta contém "depende" ou "com penalidade", você é refém.

04 Onde ficam as evidências após o fim do projeto?

Evidências em servidor do fornecedor são passivo seu. Exija retenção sob sua custódia ou destruição comprovada.

05 Se alguém do time do fornecedor agir de má-fé, o que acontece comigo?

A resposta correta contém garantia financeira e responsabilização integral do fornecedor, não do profissional.

06 Que log do que essas pessoas fizeram eu posso auditar, seis meses depois?

"Confie no nosso processo" não é uma resposta.

— § 08 · SOBRE

Sobre a intrus.io.

A intrus.io é uma empresa brasileira de segurança ofensiva fundada em Brasília, com escritórios em Portugal, Itália, Marrocos, Espanha, Estados Unidos e Austrália. 90% dos engajamentos são manuais; 10% apoiados por automação sob supervisão humana.

Certificações do time incluem OSCP, CEH, CISSP, CompTIA PenTest+, CRTO e GPEN. Frameworks de base: OWASP, MITRE ATT&CK, PTES e NIST.

Clientes selecionados: Caixa Econômica Federal (reconhecida como melhor pentest técnico em avaliação competitiva), Banco BMG, Multibanco, iFood, ArcelorMittal, Polícia Civil/Militar/Federal, CREA, Santa Casa de Misericórdia (Portugal), Fórmula 1, e instituições do ecossistema OpenFinance/OpenBanking.

AUTORIA

Este documento é de autoria de **Douglas dos Santos Lopes**, fundador e CEO da intrus.io. Revisão interna: Gabriele (Security Specialist, Roma) e Hebert. Versão 1.0, publicada em abril de 2026.

PRÓXIMO PASSO

Conversa de 30 minutos. Com o *fundador.* Sem SDR.

Você explica o escopo. A gente explica quem encaixa. Se o fit existir, começamos. Se não, você sai da conversa sabendo mais do que entrou. Esse é o piso.

Douglas Lopes · CEO, intrus.io

douglas@intrusioncyber.com
intrus.io/crivo · Brasília · Lisboa · Roma