

Da exposição à evidência.

CTEM com IA no centro.

A Hashiro conecta pentest conduzido por IA, visibilidade da superfície de ataque externa, postura de nuvem e gestão de vulnerabilidades em uma plataforma de Gestão Contínua da Exposição a Ameaças (CTEM). As equipes definem o escopo, revisam achados candidatos e mantêm as evidências conectadas à correção e ao reteste.

A IA propõe. As pessoas decidem.

Para equipes internas de segurança e prestadores de serviços de segurança que gerenciam avaliações em organizações de clientes.

<https://hashiro.ai> / hello@hashiro.ai

Um fluxo conectado de gestão da exposição

Pentest conduzido por IA

Execute avaliações com escopo definido nos modos Automatic, Assisted ou Checklist. Inspecione progresso e evidências; revise os candidatos antes de aceitar os achados. Os controles disponíveis dependem de permissões e configuração.

Superfície de ataque externa

Descubra domínios, ativos, URLs e serviços expostos. Colete metadados de tecnologias e HTTP, identifique possíveis exposições e monitore mudanças conforme a programação configurada.

Postura de nuvem

Conecte contas AWS, Azure e GCP para revisar recursos, configurações incorretas e mapeamentos aos benchmarks CIS. O acompanhamento de conformidade não constitui certificação.

Achados e relatórios

Mantenha evidências, severidade, ativos afetados e orientações de correção juntos. Acompanhe revisão, correção e reteste, mapeie cadeias de ataque e gere relatórios de projeto em PDF.

Equipes e integrações

Use ambientes restritos à organização para equipes internas e prestadores. Conecte os fluxos por sincronização com Jira, API pública e Galileo CLI.

Funcionalidades, limites, perfis de execução e plugins dependem de licença, permissões e provisionamento. Uma avaliação concluída ainda pode conter trabalho bloqueado, cobertura incompleta ou candidatos não verificados; ela não garante que o ambiente esteja seguro.

O pentest encontra um caminho. O CTEM fecha o ciclo.

01 Definir

Estabeleça escopo autorizado, exclusões e contexto do projeto.

02 Descobrir

Amplie a visibilidade dos ativos e serviços expostos.

03 Validar

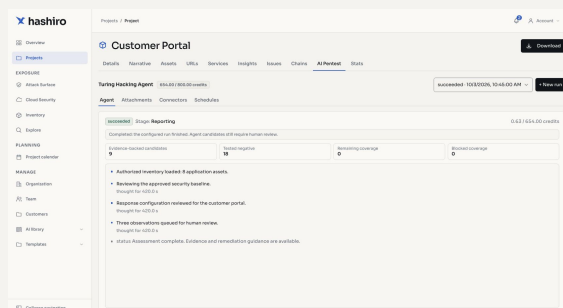
Investigue com avaliações conduzidas por IA; revise as evidências.

04 Corrigir

Mantenha status, responsáveis e orientações conectados.

05 Retestar

Verifique a correção e oriente a próxima avaliação.

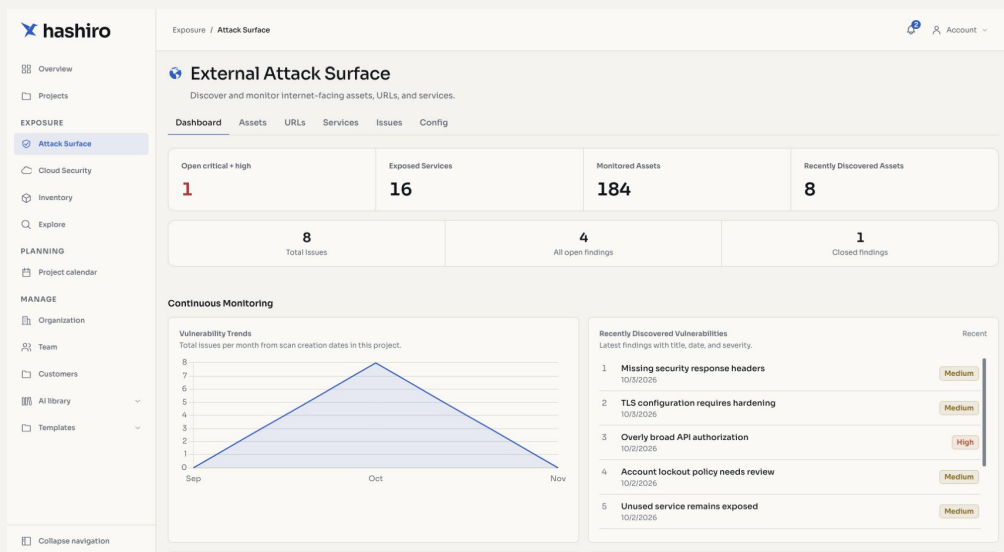


Ambiente de avaliações com IA: execuções configuradas, progresso e resultados para revisão.

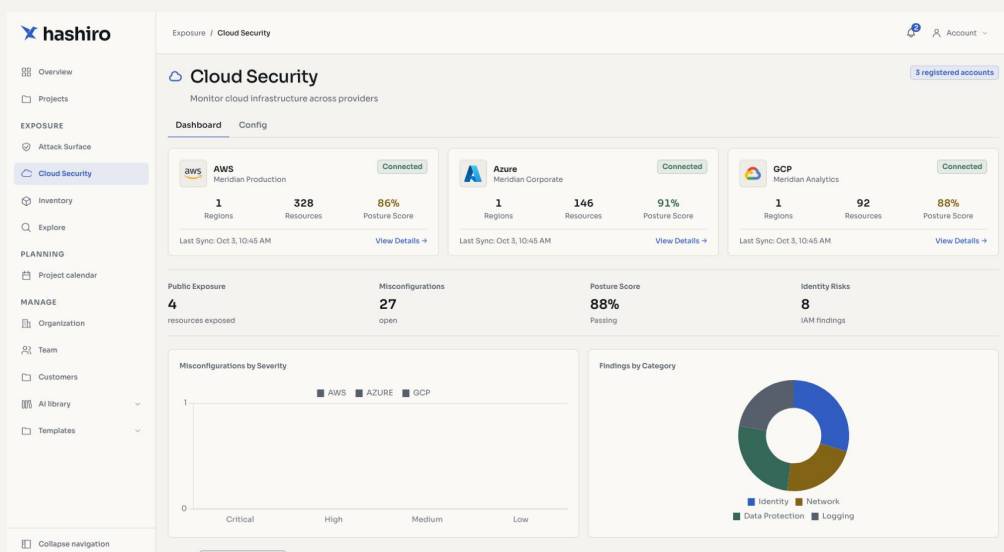
Interface real do produto com dados fictícios de demonstração. As imagens são ilustrativas, não evidências de clientes nem métricas de desempenho. As capturas incluídas estão em inglês.

Por dentro do produto

Interface real do produto com dados fictícios de demonstração. As imagens são ilustrativas, não evidências de clientes nem métricas de desempenho. As capturas incluídas estão em inglês.



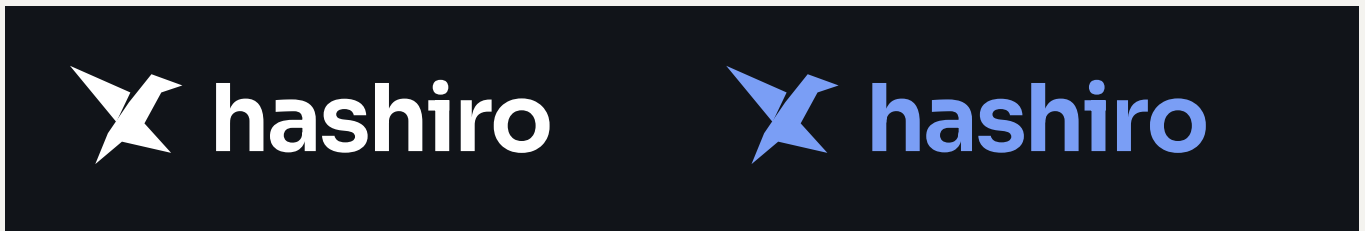
Superfície de ataque externa: ativos descobertos, serviços expostos e achados monitorados.



Postura de nuvem: contas conectadas, recursos e configurações incorretas.

Identidade Flight

Use o emblema Flight e o logotipo vetorial em letras minúsculas fornecidos. O nome do produto é Hashiro; o estilo em minúsculas pertence à arte do logotipo.



Use a versão escura sobre fundos claros e a versão branca sobre fundos escuros. Use a versão azul apenas quando houver contraste adequado.

Preserve proporções e geometria. Não redesenhe o logotipo, distorça, gire ou acrescente efeitos.

Orientação deste kit: deixe ao menos um quarto da altura do emblema como área livre. Use a assinatura completa ao apresentar a marca; use o símbolo isolado quando Hashiro já estiver identificada.

Prefira SVG para impressão e layouts escaláveis. PNGs transparentes atendem ferramentas sem suporte a SVG. A arte branca em PNG fica intencionalmente invisível sobre fundo branco.

Sora é a família tipográfica principal; JetBrains Mono é usada em rótulos técnicos. As fontes estáticas incluídas mantêm os avisos da SIL Open Font License.

Mantenha as legendas e o aviso de dados de demonstração junto às imagens. Recorte apenas quando isso não alterar o fluxo representado nem ocultar contexto relevante.

 Flight blue #7A9EF5

 Ink #111419

 Paper #F4F3EF

 White #FFFFFF

 Text blue on light #2C54C2

Textos e contato

Descrição curta

A Hashiro é uma plataforma CTEM que conecta pentest conduzido por IA, visibilidade da superfície de ataque, postura de nuvem e gestão de achados, com revisão humana no centro.

Sobre a Hashiro

A Hashiro é uma plataforma de Gestão Contínua da Exposição a Ameaças (CTEM) com pentest conduzido por IA no centro. Ela reúne descoberta da superfície de ataque externa, postura de nuvem, avaliações com escopo definido e gestão de vulnerabilidades em um ambiente conectado. Equipes de segurança e prestadores definem limites autorizados, inspecionam evidências e revisam achados candidatos antes de decidir como agir. Os achados aceitos preservam contexto dos ativos, severidade e orientações de correção ao longo do reteste e da geração de relatórios. Ambientes restritos à organização atendem programas internos e prestadores que trabalham com organizações de clientes.

Contato geral e solicitações de demonstração

hello@hashiro.ai

<https://hashiro.ai>

Descreva funcionalidades, não resultados garantidos. Não acrescente logotipos de clientes, depoimentos, selos de certificação, estatísticas de desempenho, histórico de investimentos ou biografias de fundadores sem aprovação verificada separadamente. Este kit não inclui essas comprovações.

Use estes materiais para descrever a Hashiro com precisão. A titularidade da marca permanece inalterada; o kit não concede licença geral de marca nem implica endosso. Consulte a equipe para permissões ou usos além de cobertura editorial.