

GUIA DE REFERÊNCIA

Documentação do produto

Plataforma / API / Galileo CLI

Manual para provedores e clientes



EDIÇÃO EM PORTUGUÊS

Documentação pública completa

hashiro.ai

Como usar este manual

Um guia prático para provedores e clientes da Hashiro.

01 / Comece pelo seu papel

Os guias para provedores e clientes explicam os recursos e responsabilidades de cada organização. Depois, use os capítulos da plataforma para as tarefas do dia a dia.

02 / Navegue pela referência

O sumário inclui links e números de página. Os marcadores do PDF agrupam o conteúdo por parte, capítulo e seção. Os links do manual levam diretamente ao título correspondente.

03 / Use exemplos com contexto

As capturas de tela contêm dados fictícios de demonstração. Perfis, controles e funcionalidades disponíveis dependem das permissões e da configuração da organização.

04 / Consulte as integrações

Galileo CLI e API têm partes próprias, com instalação, configuração, comandos e exemplos. A API pública usa <https://api.hashiro.ai/api/>.

05 / Mantenha a documentação atualizada

Este manual registra a versão pública da documentação. A área de Downloads do site oferece as novas edições. A documentação interna de administração não faz parte deste PDF.

Conteúdo

Selecione um capítulo ou use o número de página.

01 / Primeiros passos	5
01.01 / Introdução	6
01.02 / Início rápido	8
01.03 / Guia para provedores	11
01.04 / Guia para clientes	13
01.05 / Autenticação	15
02 / Manual da plataforma	18
02.01 / Dashboard	19
02.02 / Gestão da superfície de ataque externa (EASM)	22
02.03 / Ativos	25
02.04 / Serviços	28
02.05 / Achados	31
02.06 / Configuração do escopo	34
02.07 / Segurança em nuvem	36
02.08 / Conectar uma conta de nuvem	38
02.09 / Configurações incorretas	41
02.10 / Conformidade	44
02.11 / Projetos	46
02.12 / Gerenciamento de escopo	49
02.13 / Narrativa	51
02.14 / Cadeias de ataque	52
02.15 / Geração de relatórios	54
02.16 / Gestão de vulnerabilidades	56
02.17 / Ciclo de vida dos achados	59
02.18 / Pontuação CVSS	61
02.19 / Revisão assistida por IA	63
02.20 / Avaliações com IA	65
02.21 / Execuções de IA	68
02.22 / Execuções locais	73
02.23 / Execuções purple team	76
02.24 / Tipos de agente	79
02.25 / Avaliações automáticas	81
02.26 / Modos de execução	82
02.27 / Checklists	85

02.28 / Agendamentos de IA	87
02.29 / Conectores	89
02.30 / Base de conhecimento	91
02.31 / Créditos e cobrança	92
02.32 / Inventário	94
02.33 / Explorar	96
02.34 / Calendário de projetos	98
02.35 / Templates	100
02.36 / Templates de vulnerabilidade	101
02.37 / Templates Nuclei	103
02.38 / Templates de relatório	104
02.39 / Links de compartilhamento	106

03 / Organização e equipes 107

03.01 / Gerenciamento da organização	108
03.02 / Equipe e usuários	110
03.03 / Funções e permissões	113
03.04 / Gerenciamento de clientes	115
03.05 / Notificações	117
03.06 / Configurações	120
03.07 / Integrações	121
03.08 / Integração Jira	122

04 / Galileo CLI 125

04.01 / Galileo CLI	126
04.02 / Instalação	127
04.03 / Configuração	129
04.04 / Referência de comandos	132
04.05 / Importações	143

05 / Referência da API 144

05.01 / API Hashiro	145
05.02 / Autenticação	147
05.03 / Projetos e escopo	149
05.04 / Ativos, URLs e serviços	151
05.05 / Achados e revisão	153
05.06 / Organizações e usuários	155



PARTE 01

Primeiros passos

Conheça a plataforma, seu papel e os primeiros passos.

CAPÍTULOS / 05

01.01

Introdução

Hashiro é uma plataforma de **Gestão Contínua de Exposição a Ameaças (CTEM)** que oferece às equipes de segurança visibilidade sobre a superfície de ataque externa, a infraestrutura em nuvem e as vulnerabilidades em um único console.

Para quem é o Hashiro?

- **Equipes de segurança e SOCs:** centralização da descoberta de ativos, acompanhamento de vulnerabilidades e remediação.
- **Pentesters:** gestão completa das avaliações, com escopo, enumeração de ativos, documentação de achados, cadeias de ataque e relatórios.
- **MSSPs e provedores de segurança:** atendimento a vários clientes com isolamento entre organizações, relatórios personalizados e visão agregada dos ambientes.
- **Empresas:** visibilidade contínua sobre exposição externa e postura em nuvem sem reunir ferramentas isoladas.

Recursos principais

Gestão da superfície de ataque (EASM)

Descubra e monitore continuamente seus ativos externos. O Hashiro enumera subdomínios, consulta serviços HTTP, identifica tecnologias, captura telas e sinaliza serviços expostos conforme o agendamento definido.

Segurança em nuvem

Conecte contas AWS, Azure e GCP para detectar configurações incorretas, acompanhar conformidade com os benchmarks CIS e monitorar a postura de segurança entre provedores.

Projetos

Gerencie pentests, programas de bug bounty e revisões de segurança. Defina o escopo, acompanhe ativos, documente achados, organize cadeias de ataque e gere relatórios PDF.

Avaliações com IA

Execute avaliações de segurança com agentes de IA. Tipos de agente configuráveis definem etapas de descoberta, análise de vulnerabilidades, validação e relatório, com participação humana ou execução automática.

Gestão de vulnerabilidades

Acompanhe achados desde o rascunho até abertura, reteste, remediação e encerramento. Pontuação CVSS v3.1, trilhas de auditoria, revisão assistida por IA e verificação de candidatos mantêm a equipe alinhada.

Inventário e exploração

Pesquise ativos, URLs, serviços e achados de todos os projetos da organização. Filtre por tecnologia, servidor web, CDN e outros atributos.

Templates

Templates reutilizáveis de vulnerabilidade, verificações Nuclei e relatórios em LaTeX agilizam a produção de resultados consistentes.

Integrações

A integração bidirecional com Jira, os tokens de API, o Galileo CLI e os webhooks conectam o Hashiro aos seus fluxos de trabalho.

Organização da plataforma

Seção	Finalidade
Dashboard	Indicadores, tendências e alertas
Superfície de ataque	Descoberta e monitoramento EASM
Nuvem	Gestão da postura de segurança em nuvem
Projetos	Avaliações de segurança
Inventário	Pesquisa de ativos entre projetos
Explorar	Pesquisa textual e por expressões regulares
Calendário	Planejamento das datas dos projetos
Templates	Modelos de vulnerabilidade, Nuclei e relatórios
Biblioteca de IA	Tipos de agente, checklists, agendamentos e conectores
Organização	Equipe, funções, integrações e configurações

Isolamento entre organizações O Hashiro atende organizações **provedoras**, que gerenciam vários **clientes**, e organizações independentes. O isolamento dos dados é aplicado em todas as camadas.

Próximos passos

- [Início rápido](#): configure sua conta e execute sua primeira verificação.
- [Autenticação](#): conheça login, MFA e tokens de API.

01.02

Início rápido

Comece a usar o Hashiro em poucos minutos.

1. Entre na plataforma

Você receberá um convite por email do administrador da organização ou do provedor. Abra o link para definir sua senha e ativar a conta.

Use o [console Hashiro](#) para o convite e a configuração da conta.

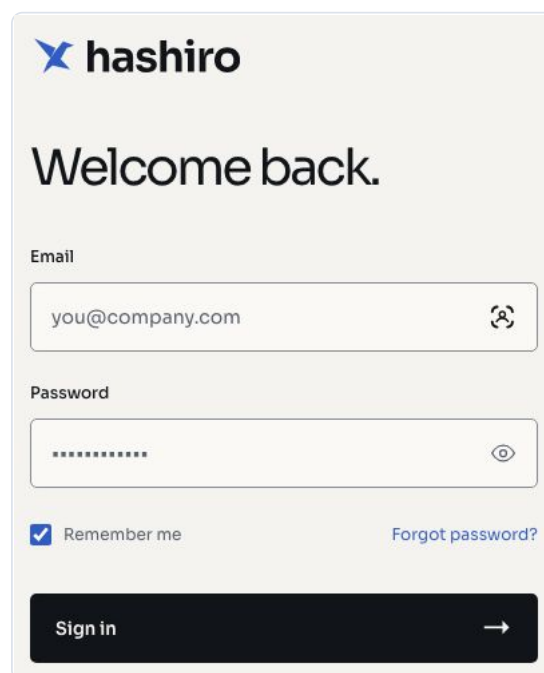


Figura 1 / Página de login do Hashiro

2. Configure a MFA

O Hashiro oferece autenticação multifator por TOTP, uma senha temporária baseada em tempo. Recomendamos ativá-la imediatamente.

1. Abra **Minha conta** no menu do usuário.
2. Acesse **Segurança**.
3. Clique em **Ativar MFA**.
4. Leia o QR code com seu aplicativo autenticador, como Google Authenticator, Authy ou 1Password.
5. Digite o código de verificação para confirmar.

Algumas organizações exigem MFA. Se a política de OTP estiver ativada, a configuração será obrigatória no primeiro acesso.

3. Explore o dashboard

O **Dashboard** é a página inicial com um resumo da postura de segurança:

- Riscos graves e vulnerabilidades em aberto em todos os projetos.
- Superfície de ataque: ativos e serviços expostos.
- Segurança em nuvem: pontuação de postura e configurações incorretas.
- Agentes de IA: execuções ativas e total de avaliações.
- Tendências de vulnerabilidades ao longo do tempo.
- Achados recentes que precisam de atenção.

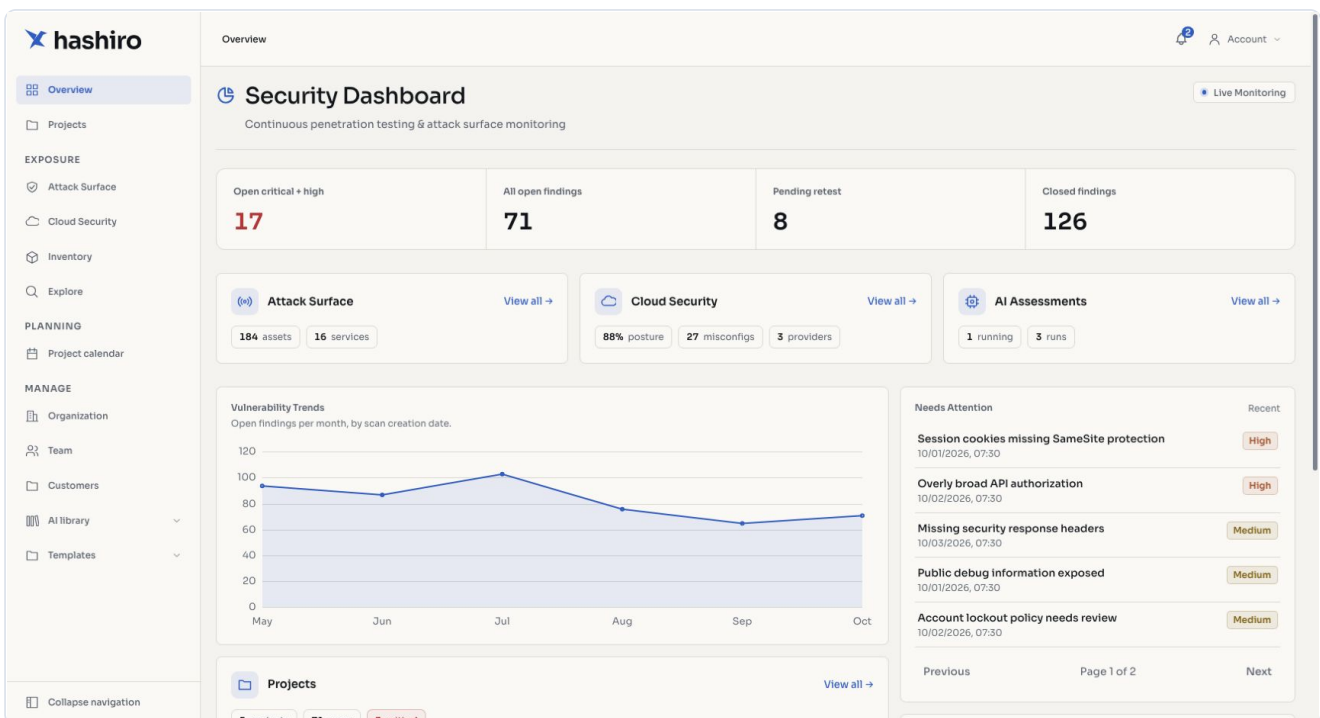


Figura 2 / Visão geral do dashboard

4. Sua primeira verificação de superfície de ataque

Se o EASM estiver habilitado para a organização:

1. Abra **Superfície de ataque** na barra lateral.
2. Acesse a aba **Configuração**.
3. Revise os alvos incluídos e adicione exclusões em **Fora do escopo**. Provedores gerenciam inclusões por padrão.
4. Salve se sua conta de provedor tiver controles de edição; caso contrário, solicite a mudança ao provedor.

Sem escopo incluído, não há monitoramento. Após a configuração, o Hashiro descobre ativos, consulta serviços e identifica achados automaticamente.

5. Crie seu primeiro projeto

Para avaliações manuais:

1. Abra **Projetos**.
2. Clique em **Novo projeto**.
3. Informe nome, tipo (caixa-preta, caixa-cinza ou caixa-branca), categoria e datas.
4. Adicione alvos dentro e fora do escopo.
5. Inclua membros da equipe e atribua funções.

Agora você pode adicionar ativos, documentar achados e construir a narrativa da avaliação.

6. Execute uma avaliação com IA

Se a organização tiver créditos de IA:

1. Abra um projeto e acesse a aba **IA**.
2. Selecione um **tipo de agente**, que define o fluxo da avaliação.
3. Escolha o **modo de execução**:
 - **Automático**: o agente trabalha de forma autônoma.
 - **Assistido**: você interage com o agente por chat.
 - **Checklist**: o agente segue uma lista de testes predefinida.
4. Inicie a execução e acompanhe o progresso em tempo real.

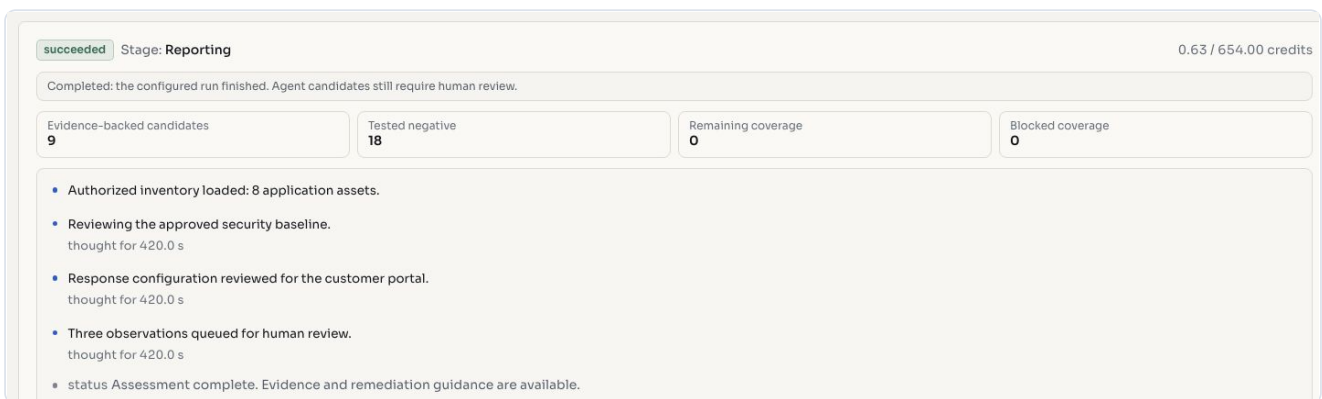


Figura 3 / Transmissão da avaliação com IA

Próximos passos

- **Dashboard**: entenda os indicadores.
- **Superfície de ataque**: conheça os recursos EASM.
- **Projetos**: aprenda a gerenciar avaliações.
- **Avaliações com IA**: configure as avaliações.
- **Equipe e usuários**: convide sua equipe.

01.03

Guia para provedores

Provedores prestam serviços a clientes vinculados. A função determina as ações disponíveis; ser provedor não concede administração global.

Configure a equipe

Em **Organização**, revise licença, nome, marca, idioma e políticas de segurança. Em **Equipe**, convide gerentes e pentesters. Gerentes administram a organização provedora; pentesters trabalham em projetos atribuídos.

Consulte [Organização](#) e [Funções](#).

Integre um cliente

Use **Clientes > Novo cliente** para provisionar a organização e convidar o usuário inicial de gerenciamento. Acompanhe o convite provisório. Antes da aceitação, há controles de convite conforme a permissão; depois, as credenciais pertencem ao cliente.

Consulte [Gerenciamento de clientes](#).

Entregue uma avaliação

Crie o projeto para o cliente autorizado, defina escopo e exclusões, atribua membros e documente achados. Revise candidatos de IA antes da publicação. Atualize a narrativa e gere o relatório quando estiver pronto.

Clientes consultam os resultados publicados sem editar a configuração dos projetos do provedor.

Consulte [Projetos](#), [Achados](#) e [Relatórios](#).

Monitoramento de superfície

Provedores gerenciam os alvos incluídos por padrão quando os controles estão disponíveis. Revise os alvos com o cliente e mantenha as exclusões. Sem alvos incluídos, não há monitoramento em execução.

Consulte [Configuração do escopo](#) e [Achados de superfície](#).

Segurança em nuvem

Oriento o cliente a conectar as próprias contas com permissões de leitura. O vínculo de provedor não concede acesso irrestrito a conexões ou credenciais de nuvem. Use somente o contexto de conta autorizado.

Consulte [Conexões](#) e [Achados de nuvem](#).

API e Galileo

Use a mesma API dos clientes: `https://api.hashiro.ai/api/`. O token determina o escopo de provedor. Configure um perfil Galileo e selecione o projeto em cada operação.

Consulte [API](#) e [Galileo](#).

01.04

Guia para clientes

Clientes trabalham na própria organização. O provedor pode entregar avaliações nesse ambiente, mas sua conta não acessa os demais clientes do provedor.

Primeiro acesso

Aceite o convite, defina a senha e configure a MFA quando exigida. Use **Minha conta** para perfil, senha, token e notificações.

Consulte [Início rápido](#) e [Autenticação](#).

Equipe e permissões

O gerente realiza as operações autorizadas de equipe. Visualizadores consultam resultados atribuídos; colaboradores de avaliações precisam das permissões correspondentes no projeto.

Consulte [Equipe](#) e [Funções](#).

Consultar avaliações

Abra **Projetos**, escolha a avaliação e consulte narrativa, ativos, achados e relatório. Projetos do provedor mantêm sua configuração sob controle do provedor. Projetos internos gerenciados pelo cliente permitem que a própria equipe mantenha os dados autorizados.

Use evidências, remediação, status e histórico para coordenar correções e retestes. Candidatos públicos de IA podem precisar de revisão antes da confirmação.

Consulte [Ciclo de vida](#) e [Revisão com IA](#).

Superfície de ataque

Abra **Superfície de ataque** para consultar ativos, serviços e achados. Revise o escopo com o provedor. A seção **Fora do escopo** permanece disponível para exclusões, com edição conforme as permissões. Sem alvos incluídos, não há monitoramento em execução.

Consulte [Escopo](#) e [Status dos achados](#).

Nuvem e achados

Conecte sua conta AWS, Azure ou GCP com credenciais de leitura. Diferencie o estado da conexão dos resultados da avaliação. Abra uma configuração incorreta para consultar o recurso e a remediação e use o seletor Aberto, Resolvido ou Suprimido.

Consulte [Conectar conta de nuvem](#) e [Gerenciar achados](#).

Automação

A conexão API e Galileo usa `https://api.hashiro.ai/api/` com seu token. Um perfil basta. Operações dependem da organização e das permissões do projeto.

Consulte [API](#), [Configuração Galileo](#) e [Avaliações automáticas](#).

01.05

Autenticação

O Hashiro oferece sessões interativas para o console web e tokens de API para acesso programático.

Login no console web

Email e senha

Entre com seu email e senha. Sua sessão permanece ativa enquanto você usa o console.

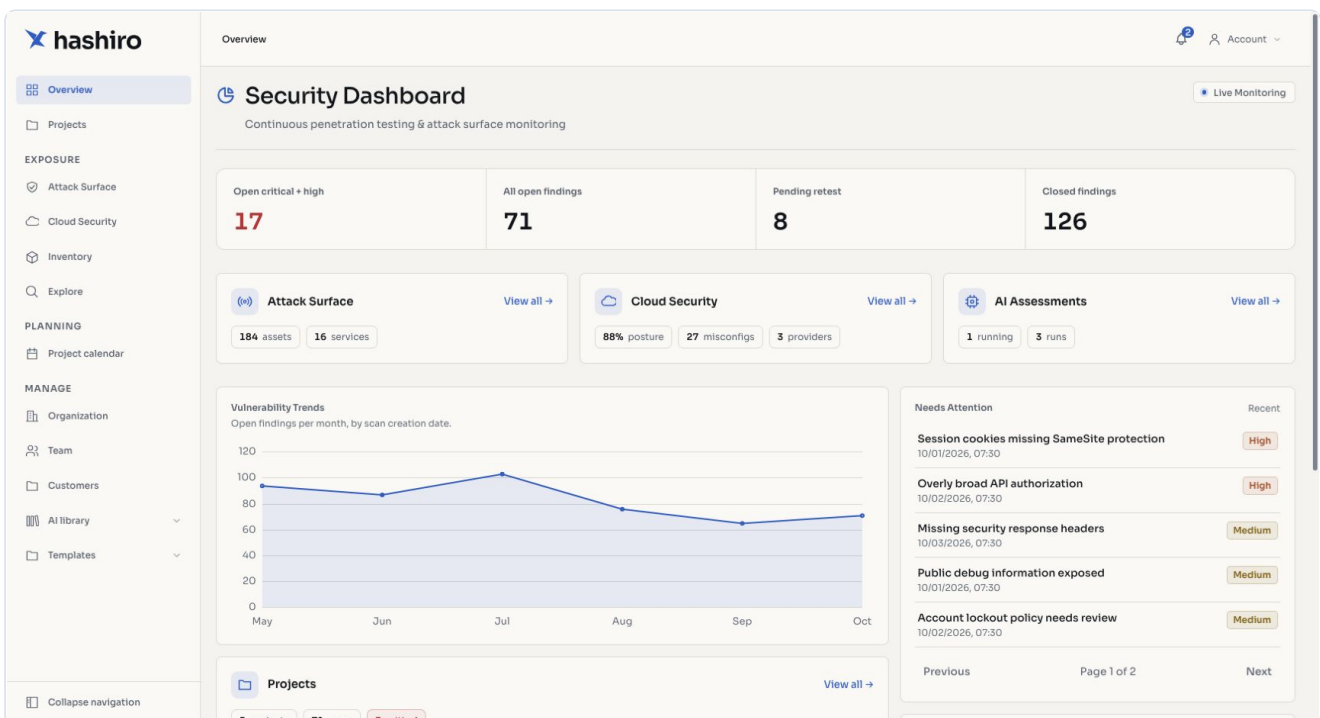


Figura 4 / Dashboard após o login

Autenticação multifator (MFA)

A MFA usa TOTP e é compatível com Google Authenticator, Authy, 1Password e aplicativos semelhantes.

Para configurar:

1. Abra **Minha conta** no menu do usuário.
2. Acesse a seção de segurança.
3. Clique em **Ativar MFA**.
4. Leia o QR code com o aplicativo autenticador.
5. Digite o código de seis dígitos para confirmar.

Depois de ativada, a plataforma solicita o código TOTP após a senha em cada login.

MFA obrigatória na organização Administradores podem ativar uma política de OTP para todos os membros. No próximo login, os usuários serão direcionados à configuração da MFA.

Gerenciamento:

- **Desativar:** desligue a MFA em Minha conta, se a política da organização permitir.
- **Redefinir:** gere um novo segredo de MFA caso tenha perdido acesso ao autenticador.

Gerenciamento de senhas

- **Alterar senha:** use Minha conta a qualquer momento.
- **Recuperar senha:** clique em “Esqueceu a senha?” no login para receber um email.
- **Primeiro acesso:** usuários provisionados por um administrador precisam definir uma nova senha.

Limites de tentativas Login, validação de OTP e recuperação de senha têm limites de requisições contra tentativas de força bruta. Após várias falhas, aguarde antes de tentar novamente.

Tokens de API

Para scripts, pipelines CI/CD, ferramentas CLI e integrações, use um token de API.

Gerar um token

1. Abra **Minha conta**.
2. Clique em **Gerar chave de API**.
3. Copie o token e armazene-o com segurança. Ele não será exibido novamente.

Usar o token

Envie o token no cabeçalho X-HASHIRO-TOKEN em cada requisição:

```
curl -H "X-HASHIRO-TOKEN: your-token-here" \  
https://api.hashiro.ai/api/projects
```

O token herda as permissões do usuário que o gerou. Todas as ações são atribuídas a esse usuário.

Autenticação no Galileo CLI

O [Galileo CLI](#) usa tokens de API configurados nos perfis TOML. Consulte [Configuração do CLI](#).

Ciclo de vida da sessão

Evento	Comportamento
Login	Emite cookies HTTP-only access_token de curta duração e refresh_token de longa duração
Expiração	Renova o acesso automaticamente com o refresh token
Logout	Limpa os dois cookies
MFA obrigatória	Direciona à verificação OTP após validar a senha

Evento	Comportamento
Primeiro acesso	Exige alteração da senha antes de liberar acesso

Considerações de segurança

- Endpoints de autenticação usam HTTPS.
- Senhas são armazenadas como hashes, nunca em texto simples.
- Tokens de API são armazenados como hashes e exibidos em texto simples apenas na geração.
- Limites de requisições protegem os endpoints de autenticação.
- A configuração de proxies confiáveis preserva a identificação correta do IP atrás de balanceadores.



PARTE 02

Manual da plataforma

Navegue pelo ambiente, revise achados e acompanhe avaliações.

CAPÍTULOS / 39

02.01

Dashboard

O dashboard oferece uma visão unificada, em tempo real, da postura de segurança da sua organização. Ele reúne métricas de superfície de ataque, segurança em nuvem, gestão de vulnerabilidades e avaliações com IA.

Os dados são atualizados automaticamente a cada 60 segundos e quando você retorna à aba do navegador.

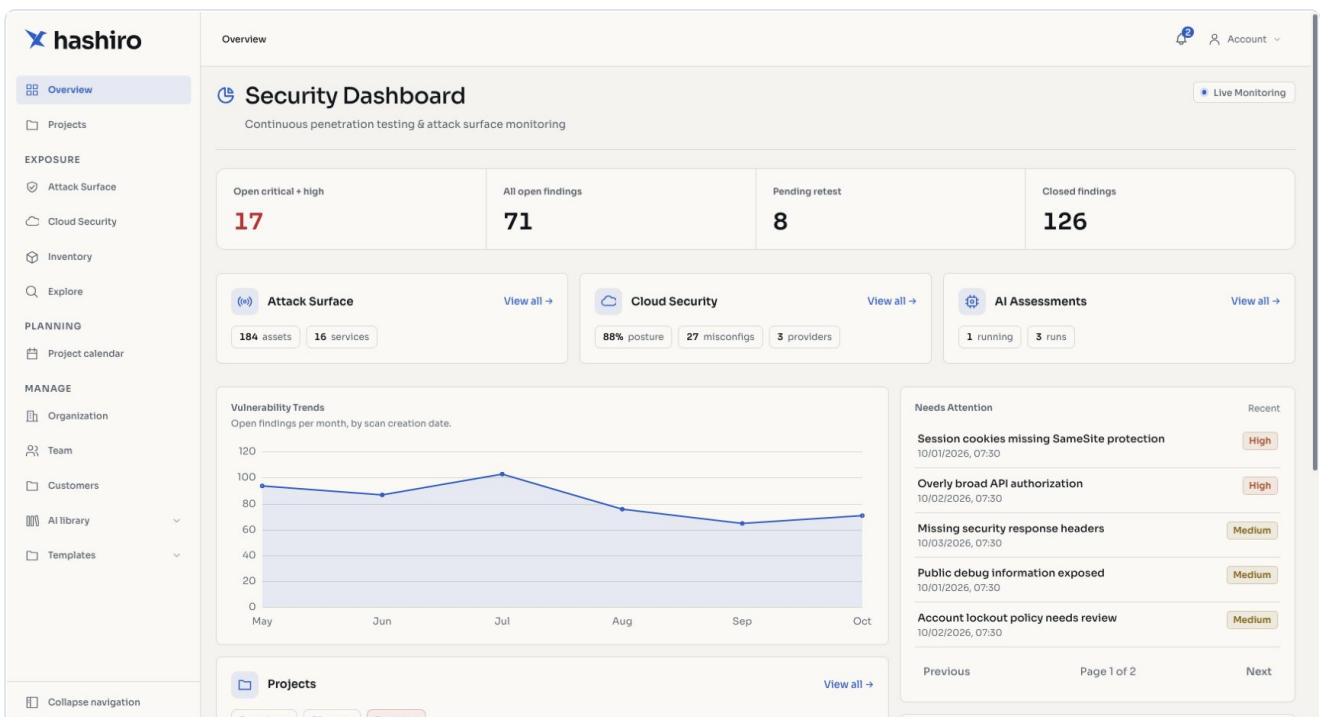


Figura 5 / Visão geral do dashboard

Indicadores de desempenho

Quatro indicadores apresentam um resumo da situação:

Indicador	Descrição
Riscos graves em aberto	Vulnerabilidades críticas e altas abertas em todos os projetos
Vulnerabilidades em aberto	Total de achados abertos, independentemente da severidade
Retestes pendentes	Achados aguardando validação após uma correção informada
Vulnerabilidades resolvidas	Achados cuja correção foi confirmada

Cartões do ambiente

Abaixo dos indicadores, três cartões resumem as principais áreas.

Superfície de ataque

- **Ativos:** total de ativos descobertos e monitorados pelo EASM.
- **Serviços expostos:** serviços visíveis na internet, com portas abertas.
- **Riscos em aberto:** achados ainda não resolvidos na superfície de ataque.

Segurança em nuvem

- **Pontuação de postura:** resultado agregado das contas de nuvem conectadas.
- **Configurações incorretas:** total de configurações incorretas em aberto.
- **Provedores:** quantidade de contas AWS, Azure e GCP conectadas.

Agentes de IA

- **Em execução:** avaliações em andamento.
- **Total de execuções:** quantidade acumulada de avaliações realizadas.

Tendências de vulnerabilidades

Um gráfico de linhas apresenta a quantidade de vulnerabilidades por mês e por severidade. Use-o para acompanhar a evolução da postura de segurança.



Figura 6 / Gráfico de tendências de vulnerabilidades

Principais projetos

Lista os projetos com mais vulnerabilidades, com indicadores por severidade, para identificar quais avaliações precisam de mais atenção.

Requer atenção

Uma lista paginada apresenta vulnerabilidades recentes que precisam de revisão, destacando achados novos ou cuja severidade aumentou.

Achados abertos por severidade

Um gráfico de barras distribui os achados abertos entre crítico, alto, médio, baixo, informativo e desconhecido.

Detalhes de remediação

Uma seção expansível oferece análises adicionais:

- **Matriz de esforço:** relaciona prioridade e complexidade dos achados em quadrantes para orientar a correção por impacto e esforço.
- **Distribuição por idade:** mostra há quanto tempo as vulnerabilidades estão abertas. Achados antigos podem indicar gargalos na remediação.
- **Estatísticas da superfície de ataque:** resume ativos, serviços e a proporção entre escopo monitorado e não monitorado.

Disponibilidade por licença

As seções do dashboard dependem da licença da organização. Recursos não incluídos no plano exibem uma opção de upgrade. Consulte seu provedor ou a equipe comercial do Hashiro para conhecer os planos.

02.02

Gestão da superfície de ataque externa (EASM)

O EASM oferece visibilidade contínua dos ativos da organização expostos à internet. O Hashiro descobre subdomínios, serviços e URLs, coleta seus dados e monitora alterações, vulnerabilidades e configurações incorretas.

É um dos pilares da **Gestão Contínua de Exposição a Ameaças (CTEM)**: o monitoramento recorrente permite identificar novas exposições conforme aparecem.

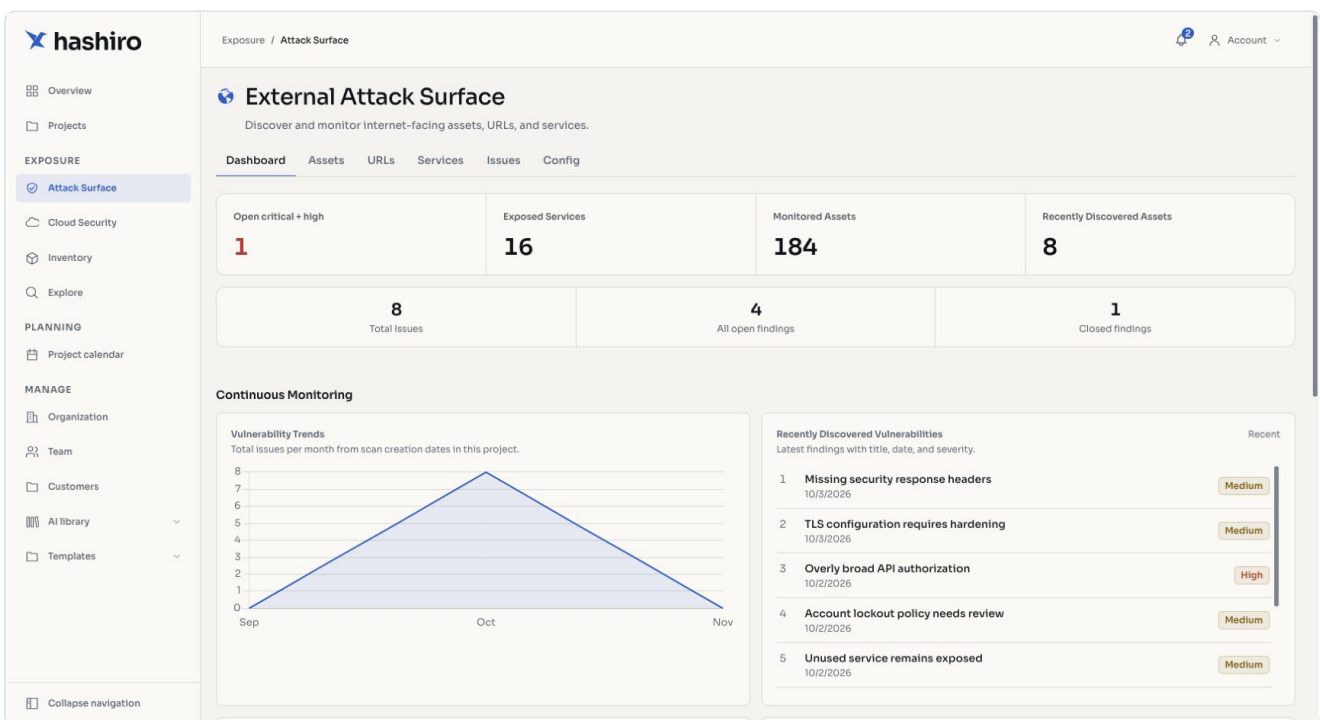


Figura 7 / Visão geral do EASM

Como funciona

- Definição do escopo:** informe domínios, IPs, CIDRs e curingas dentro e fora do escopo.
- Descoberta automática:** enumeração de subdomínios, descoberta de URLs e identificação de serviços abertos.
- Coleta de dados:** o HTTPX consulta os ativos e registra status HTTP, título, tecnologias via Wappalyzer, capturas de tela, hashes de favicon, servidor web e CDN.
- Verificação de vulnerabilidades:** templates Nuclei detectam CVEs conhecidas, configurações incorretas e exposições.
- Monitoramento contínuo:** as verificações se repetem conforme o agendamento. Ativos novos, removidos e mudanças de status são acompanhados.

Abas do módulo

Aba	Finalidade
Estatísticas	Resumo da superfície de ataque
Ativos	Lista paginada com dados de consulta, capturas e tecnologias
URLs	Caminhos descobertos e informações de consulta
Serviços	Serviços de rede identificados por verificação de portas
Achados	Vulnerabilidades e configurações incorretas
Configuração	Alvos incluídos e exclusões

Recursos principais

- **Descoberta de ativos:** enumeração automática de subdomínios e identificação de ativos.
- **Consulta HTTP:** títulos, cabeçalhos, códigos de status, tecnologias e capturas de tela.
- **Verificação de portas:** detecção de serviços expostos em 27 portas padrão.
- **Detecção de vulnerabilidades:** verificações Nuclei para CVEs, configurações incorretas e exposições.
- **Capturas de tela:** identificação visual rápida dos ativos web.
- **Tecnologias:** identificação de frameworks e bibliotecas com Wappalyzer.
- **CDNs:** identificação dos provedores à frente dos ativos.
- **Histórico de alterações:** disponibilidade, tecnologias e novas exposições ao longo do tempo.
- **Exportação:** download de dados em PDF ou CSV.

A disponibilidade e os limites EASM dependem do serviço provisionado e da licença.

Recursos relacionados

- [Segurança em nuvem](#): monitore também sua infraestrutura em nuvem.
- [Inventário](#): pesquise ativos entre projetos.

Navegar pela superfície

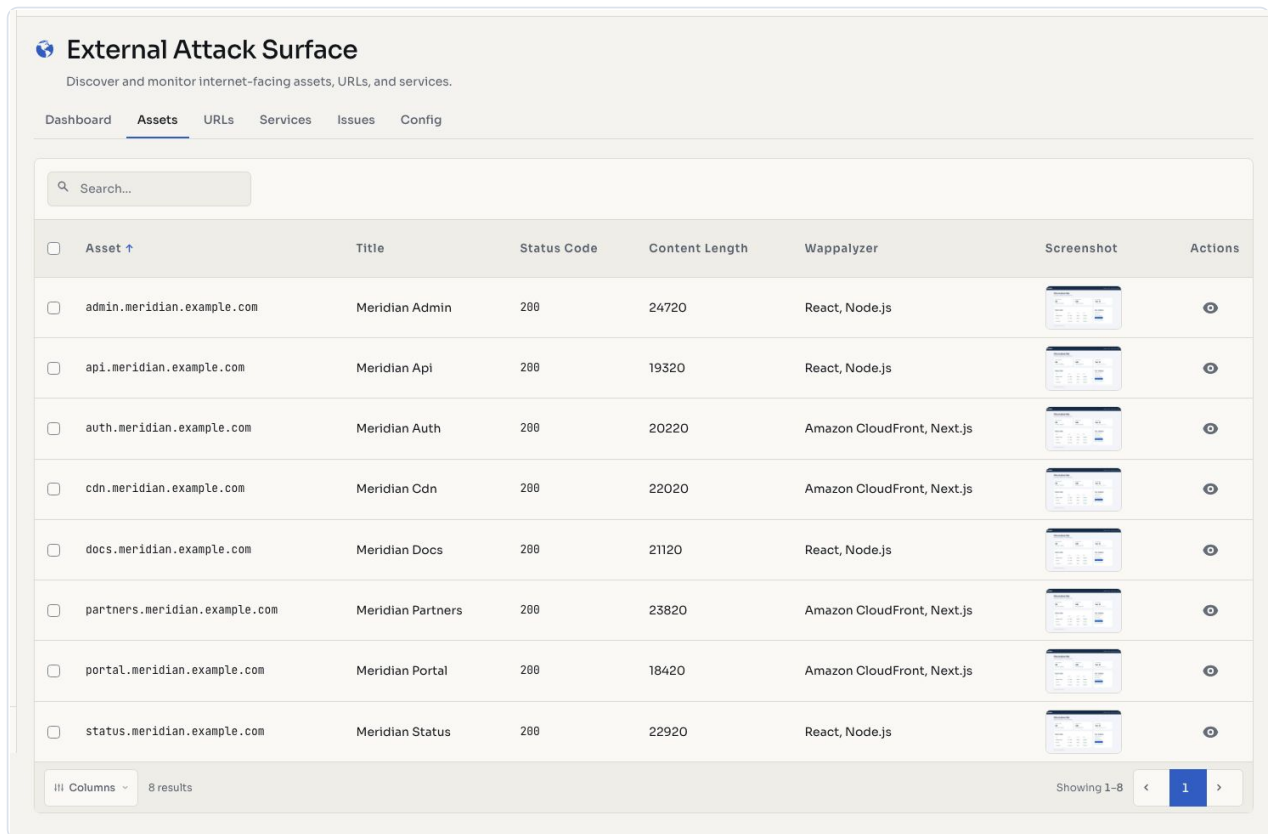
1. Abra **Superfície de ataque** na barra lateral.
2. Use **Estatísticas** para o resumo, **Ativos** para hosts, **URLs** para caminhos e **Serviços** para portas.
3. Abra uma linha para ver evidências e achados relacionados.
4. Use **Achados** para filtrar resultados e **Configuração** para consultar o escopo.

A visão é limitada à organização autorizada. Resultados vazios podem indicar ausência de escopo ou dados ainda não coletados. Consulte [Configuração do escopo](#).

02.03

Ativos

A aba Ativos apresenta os hosts e subdomínios descobertos na superfície de ataque. Cada ativo recebe dados coletados automaticamente nas verificações EASM.



The screenshot shows the 'External Attack Surface' dashboard with the 'Assets' tab selected. It displays a table of discovered assets for 'meridian.example.com'. The table includes columns for Asset, Title, Status Code, Content Length, Wappalyzer, Screenshot, and Actions. There are 8 results shown, each with a checkbox, a thumbnail screenshot, and an eye icon in the Actions column.

Asset	Title	Status Code	Content Length	Wappalyzer	Screenshot	Actions
☐ admin.meridian.example.com	Meridian Admin	200	24720	React, Node.js		
☐ api.meridian.example.com	Meridian Api	200	19320	React, Node.js		
☐ auth.meridian.example.com	Meridian Auth	200	20220	Amazon CloudFront, Next.js		
☐ cdn.meridian.example.com	Meridian Cdn	200	22020	Amazon CloudFront, Next.js		
☐ docs.meridian.example.com	Meridian Docs	200	21120	React, Node.js		
☐ partners.meridian.example.com	Meridian Partners	200	23820	Amazon CloudFront, Next.js		
☐ portal.meridian.example.com	Meridian Portal	200	18420	Amazon CloudFront, Next.js		
☐ status.meridian.example.com	Meridian Status	200	22920	React, Node.js		

Figura 8 / Lista de ativos EASM

Lista de ativos

Os ativos aparecem em uma tabela paginada:

Coluna	Descrição
Ativo	Hostname, endereço IP ou domínio
Tipo	Domínio, IP, curinga ou CIDR
Título	Título da página HTML coletado na consulta
Código de status	Resposta HTTP, como 200, 301 ou 403
Tecnologias	Frameworks, CMS, bibliotecas e linguagens identificados pelo Wappalyzer
Servidor web	Software como nginx, Apache ou Cloudflare

Coluna	Descrição
CDN	Provedor de CDN identificado, quando houver
Disponibilidade	Indica se o ativo está acessível

Dados coletados

Ativos web são consultados pelo HTTPX, que coleta:

- Código de status HTTP e cabeçalhos da resposta.
- Título da página HTML.
- Tamanho do conteúdo e hash do corpo para detectar alterações.
- Hash do favicon para identificar aplicações conhecidas.
- Hash JARM, uma impressão digital TLS do servidor.
- Tecnologias identificadas pelo Wappalyzer.
- Servidor web identificado nos cabeçalhos.
- Provedor de CDN.
- Endereços IP resolvidos para o hostname.
- Contagem de palavras e linhas.
- Capturas de tela com navegador sem interface gráfica.

Capturas de tela

O Hashiro captura a tela de cada ativo web durante a consulta. Miniaturas aparecem na lista e a imagem completa fica nos detalhes. Elas ajudam a identificar páginas de login, APIs, páginas padrão de servidores e aplicações.

Filtros e pesquisa

- **Pesquisa:** texto livre nos nomes dos ativos.
- **Tipo:** domínio, IP, curinga ou CIDR.
- **Disponibilidade:** ativos acessíveis ou indisponíveis.
- **Escopo:** dentro ou fora do escopo.

Ações

- **Copiar:** copie nomes de ativos para outras ferramentas.
- **Excluir:** remova ativos do inventário.
- **Download:** exporte a lista em PDF ou CSV.
- **Consultar novamente:** atualize os metadados dos ativos selecionados.

Detalhes do ativo

Clique em um ativo para ver:

- Captura de tela completa.
- Resposta HTTP, com cabeçalhos, status e conteúdo.
- Tecnologias identificadas.
- Resolução de endereços IP.
- Caminhos de URL associados.
- Serviços e portas associados.
- Achados relacionados ao ativo.

The screenshot displays the Hashiro platform interface for an asset named `portal.meridian.example.com`. The interface is organized into several sections:

- Navigation:** Includes a "Back to results" link and tabs for "Overview", "Services", and "URLs".
- Asset Overview:** Shows the asset name, a status indicator (Available), and a link to "Open observed host in a new tab".
- Screenshot:** Displays a screenshot of the website, which includes a welcome message for "Alex" and a table of recent orders.
- Asset Information:** Provides details about the asset, including its IP addresses (`198.51.100.20`) and tags (`environment: production`, `owner: Platform Engineering`).
- HTTP Response:** Shows the status code (`200`), content length (`18.0 KB`), page title (`Meridian Portal`), and web server (`CloudFront`).
- Technologies Detected:** Lists detected technologies, including `Amazon CloudFront` and `Next.js`.
- HTTP Headers:** Displays the content type (`text/html; charset=utf-8`) and strict transport security (`max-age=31536000`).

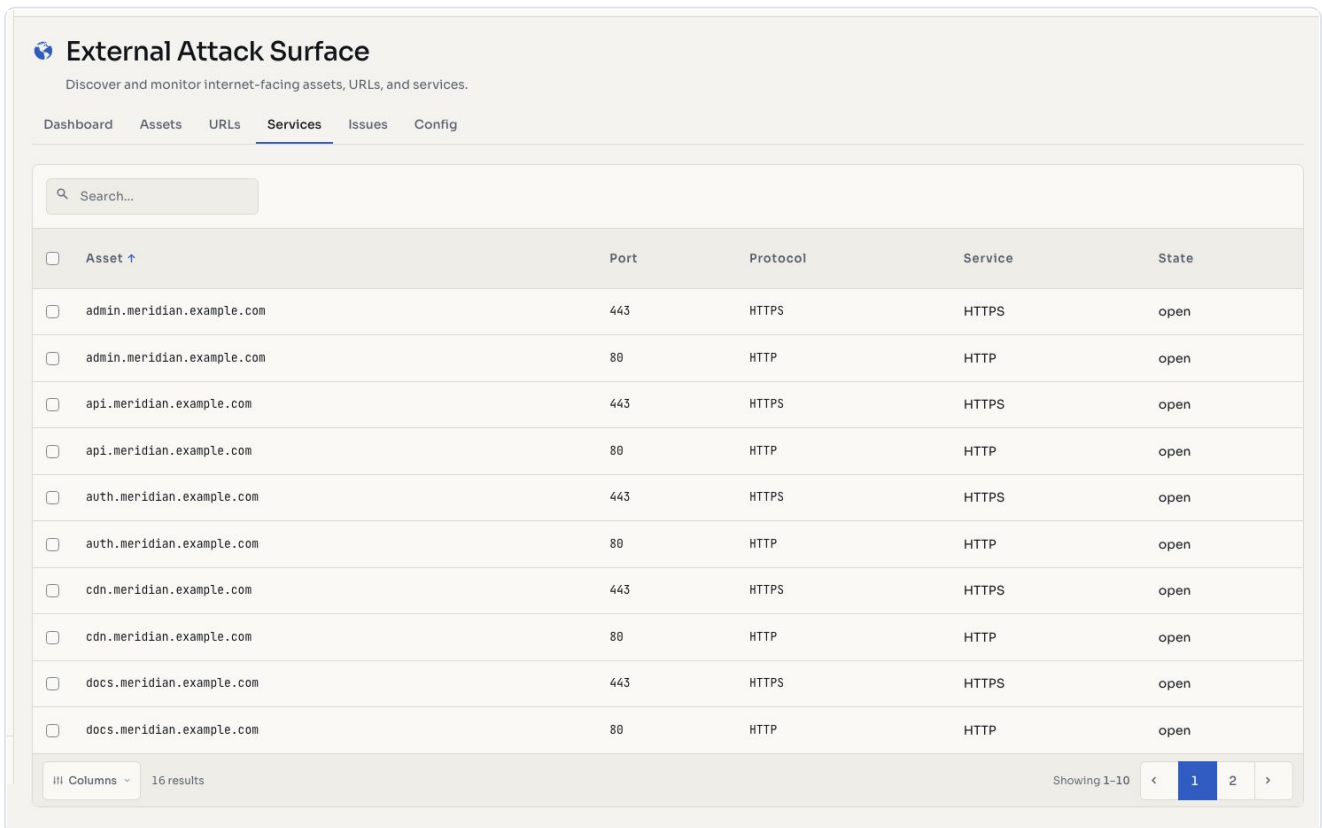
Figura 9 / Detalhes de um ativo

Os ativos são consultados novamente em cada ciclo. Você também pode solicitar uma nova consulta manual para obter dados atualizados imediatamente.

02.04

Serviços

A aba Serviços mostra os serviços de rede descobertos na superfície de ataque. Identifique portas abertas, serviços em execução e exposições inesperadas.



The screenshot shows the 'External Attack Surface' (EASM) interface. At the top, there's a search bar and navigation tabs: Dashboard, Assets, URLs, Services (selected), Issues, and Config. Below the search bar is a table with columns: Asset, Port, Protocol, Service, and State. The table lists 16 results for various domains like admin.meridian.example.com, api.meridian.example.com, auth.meridian.example.com, cdn.meridian.example.com, and docs.meridian.example.com. Each domain has two entries for ports 443 and 80, with services listed as HTTPS and HTTP. All states are 'open'. At the bottom, there's a pagination bar showing 'Showing 1-10' and page numbers 1, 2, and a next button.

Asset	Port	Protocol	Service	State
admin.meridian.example.com	443	HTTPS	HTTPS	open
admin.meridian.example.com	80	HTTP	HTTP	open
api.meridian.example.com	443	HTTPS	HTTPS	open
api.meridian.example.com	80	HTTP	HTTP	open
auth.meridian.example.com	443	HTTPS	HTTPS	open
auth.meridian.example.com	80	HTTP	HTTP	open
cdn.meridian.example.com	443	HTTPS	HTTPS	open
cdn.meridian.example.com	80	HTTP	HTTP	open
docs.meridian.example.com	443	HTTPS	HTTPS	open
docs.meridian.example.com	80	HTTP	HTTP	open

Figura 10 / Lista de serviços EASM

Descoberta de serviços

O Hashiro verifica 27 portas padrão nos ativos dentro do escopo. Exemplos:

Porta	Serviço comum
21	FTP
22	SSH
23	Telnet
25	SMTP
53	DNS
80, 443	HTTP / HTTPS

Porta	Serviço comum
110, 143, 993, 995	Email, POP3 e IMAP
3306	MySQL
3389	RDP
5432	PostgreSQL
6379	Redis
8080, 8443	HTTP / HTTPS alternativos
27017	MongoDB

Bancos de dados e serviços de acesso remoto expostos à internet são sinalizados como alto risco. Revise-os imediatamente e restrinja o acesso à rede interna ou VPN.

Tabela de serviços

Coluna	Descrição
Ativo	Hostname ou IP do serviço
Porta	Número da porta
Protocolo	TCP ou UDP
Estado	open, filtered ou closed
Serviço	Nome identificado, como http, ssh ou mysql

Estados das portas

- **Aberta:** aceita conexões e tem um serviço em execução.
- **Filtrada:** bloqueada por firewall, sem determinação do estado.
- **Fechada:** acessível, mas sem serviço escutando.

Análise da exposição de rede

Use a visualização para identificar bancos de dados expostos, interfaces administrativas públicas como SSH e RDP, serviços inesperados ou antigos e aplicações em portas não convencionais.

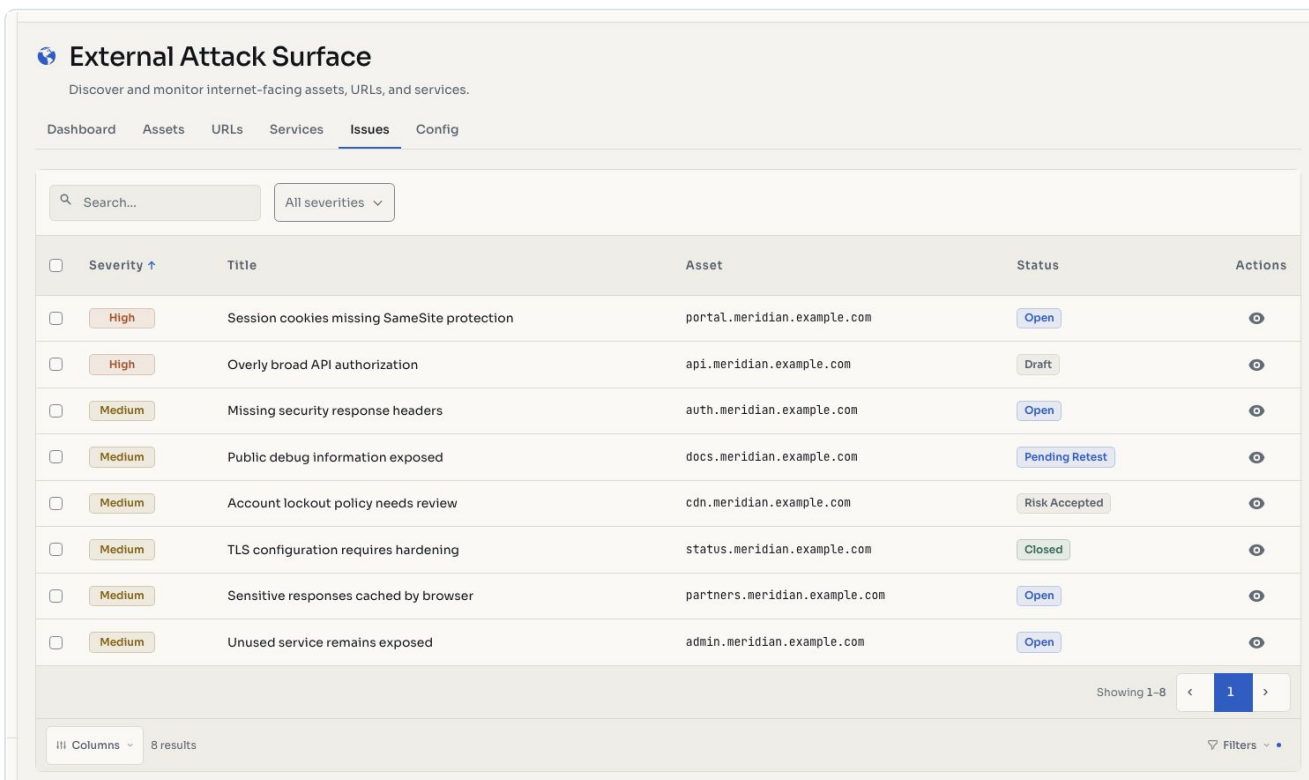
Ações

- **Filtrar por estado:** portas abertas, filtradas ou fechadas.
- **Filtrar por porta:** procure números específicos.
- **Abrir ativo:** acesse os detalhes completos do ativo.

02.05

Achados

A aba Achados mostra vulnerabilidades e configurações incorretas detectadas automaticamente nas verificações EASM, por templates Nuclei e outros mecanismos.



The screenshot displays the 'External Attack Surface' dashboard with the 'Issues' tab selected. It shows a table of 8 detected issues, each with a severity level, title, asset, status, and actions. The issues include 'Session cookies missing SameSite protection' (High), 'Overly broad API authorization' (High), 'Missing security response headers' (Medium), 'Public debug information exposed' (Medium), 'Account lockout policy needs review' (Medium), 'TLS configuration requires hardening' (Medium), 'Sensitive responses cached by browser' (Medium), and 'Unused service remains exposed' (Medium). The status of these issues varies, including 'Open', 'Draft', 'Pending Retest', 'Risk Accepted', and 'Closed'.

Severity	Title	Asset	Status	Actions
High	Session cookies missing SameSite protection	portal.meridian.example.com	Open	
High	Overly broad API authorization	api.meridian.example.com	Draft	
Medium	Missing security response headers	auth.meridian.example.com	Open	
Medium	Public debug information exposed	docs.meridian.example.com	Pending Retest	
Medium	Account lockout policy needs review	cdn.meridian.example.com	Risk Accepted	
Medium	TLS configuration requires hardening	status.meridian.example.com	Closed	
Medium	Sensitive responses cached by browser	partners.meridian.example.com	Open	
Medium	Unused service remains exposed	admin.meridian.example.com	Open	

Figura 11 / Lista de achados EASM

Lista de achados

Coluna	Descrição
Título	Nome da vulnerabilidade ou configuração incorreta
Ativo	Hostname ou IP afetado
Severidade	Crítico, alto, médio, baixo ou informativo
Status	Estado atual, como aberto ou fechado
Deteção	Data da primeira identificação

Níveis de severidade

- **Crítico:** vulnerabilidade explorável de impacto grave, como execução remota de código ou desvio de autenticação.
- **Alto:** risco significativo de exposição de dados ou comprometimento de sistemas.
- **Médio:** risco moderado para o ciclo regular de correção.
- **Baixo:** problema menor com impacto direto limitado.
- **Informativo:** observação útil para reforçar a segurança, sem risco direto.

Detecção automática

- **Templates Nuclei:** verificações comunitárias e personalizadas para CVEs, configurações incorretas, credenciais padrão e painéis expostos.
- **Verificações de configuração:** cabeçalhos de segurança ausentes, TLS inseguro e redirecionamentos abertos.
- **Detecção de exposição:** arquivos sensíveis, backups, listagens de diretórios e endpoints de depuração.

Operações em lote

Selecione vários achados para alterar o status para aberto, fechado, aceito ou não aplicável, conforme as permissões disponíveis.

Detalhes do achado

Clique em um achado para abri-lo na [Gestão de vulnerabilidades](#). Você pode revisar descrição e evidências, atribuir CVSS, acompanhar remediação, registrar retestes e consultar histórico e auditoria.

Achados EASM seguem o mesmo ciclo de vida, status e recursos de relatório dos achados manuais. A diferença está na detecção automática.

Recursos relacionados

- [Gestão de vulnerabilidades](#): ciclo de vida e remediação.
- [Templates Nuclei](#): personalize as verificações.
- [Configuração EASM](#): alvos incluídos e exclusões.

Alterar o status dos achados

A organização acompanha a remediação com os controles de status disponíveis à conta.

1. Abra **Superfície de ataque > Achados**.
2. Pesquise ou filtre os registros.
3. Abra um achado para revisar descrição, ativo, evidências e histórico.

4. Para vários registros, selecione as linhas e escolha **Alterar status**.
5. Escolha o status, confirme e confira a tabela.

As opções incluem **Aberto**, **Fechado**, **Inválido**, **Fora do escopo**, **Risco aceito**, **Em revisão** e **Reteste pendente**. Rascunho fica disponível para provedores elegíveis. Use Reteste pendente quando a correção precisar de verificação e Fechado após confirmação. Risco aceito documenta a decisão consciente de manter o risco.

Mudar o status registra uma decisão, sem corrigir o sistema afetado. Se não puder editar, confira organização e função com o gerente. Candidatos de IA podem exigir o fluxo específico de revisão.

02.06

Configuração do escopo

Abra **Superfície de ataque > Configuração** para consultar os alvos monitorados e as exclusões da organização.

Scope and context

Scope Out of Scope

In Scope Add Line

Asset	Asset Type	Actions
*.meridian.example.com	domain	
api.meridian.example.com	domain	
198.51.100.0/24	cdir	

Copy to clipboard

Figura 12 / Configuração da superfície de ataque

Alvos dentro do escopo

Por padrão, **provedores gerenciam os alvos dentro do escopo**. Se sua conta tiver os controles disponíveis, adicione, edite ou remova os alvos autorizados. Clientes consultam o escopo e solicitam alterações ao provedor quando não podem editar.

Tipo	Exemplo
Domínio	example.com
Curinga	*.example.com
Endereço IP	203.0.113.10
Intervalo CIDR	203.0.113.0/24

1. Abra **Dentro do escopo**.
2. Adicione uma linha e selecione o tipo.

3. Informe domínio, curinga, IP ou intervalo.
4. Salve e confira a lista.

Inclua somente alvos autorizados. Os controles de edição dependem das permissões e do provisionamento do serviço.

Sem escopo, sem monitoramento

Uma lista vazia de alvos incluídos significa que o monitoramento **não está executando contra nenhum alvo**. Uma exclusão sozinha não inicia o serviço. Se não houver escopo, solicite ao provedor a definição dos alvos.

Alvos fora do escopo

A seção **Fora do escopo** está sempre disponível na visão de superfície da organização para definir exclusões. Os controles de escrita ainda dependem das permissões.

1. Abra **Configuração > Fora do escopo**.
2. Adicione o alvo excluído e escolha o tipo.
3. Salve.
4. Confira a entrada na lista.

Exclusões têm prioridade sobre inclusões. Use-as para sistemas de terceiros, alvos sensíveis ou ambientes que não devem ser verificados. Altere ou remova uma exclusão somente quando a autorização mudar.

Consultar resultados

Alterações no escopo não substituem resultados imediatamente. Consulte [Ativos](#), [Serviços](#) e [Achados](#) para visualizar dados e gerenciar resultados. Registros históricos podem continuar visíveis após uma exclusão.

02.07

Segurança em nuvem

O módulo oferece **Gestão da Postura de Segurança em Nuvem (CSPM)**: monitoramento contínuo de configurações incorretas, lacunas de conformidade e riscos.

Conecte contas AWS, Azure ou GCP para verificar recursos e acompanhar a evolução da postura de segurança.

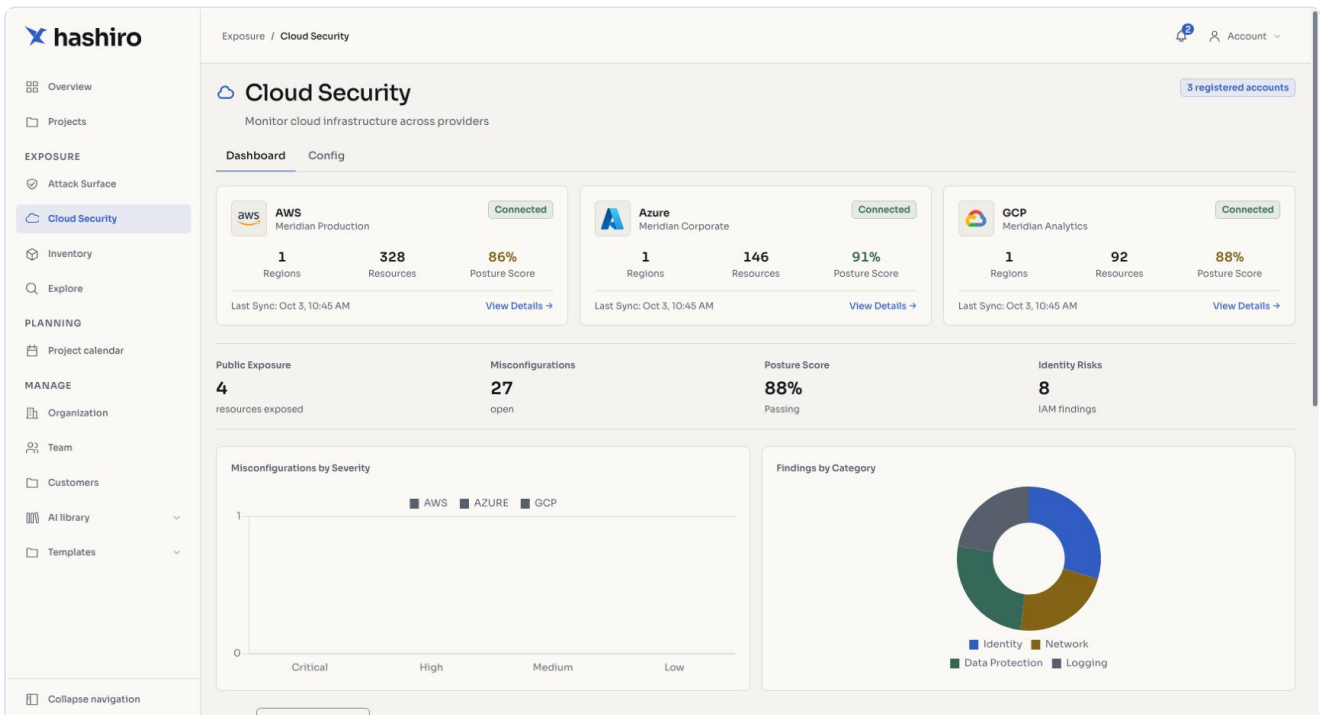


Figura 13 / Dashboard de segurança em nuvem

Suporte a múltiplas nuvens

Provedor	Método de conexão
AWS	Credenciais de chave de acesso no formulário atual
Azure	Credenciais de entidade de serviço
GCP	Chave de conta de serviço

Conecte várias contas de diferentes provedores para uma visão unificada do ambiente.

Dashboard de nuvem

- **Pontuação de postura:** resultado agregado das contas conectadas.
- **Recursos:** total de recursos descobertos e monitorados.

- **Configurações incorretas:** achados abertos por severidade.
- **Exposição pública:** recursos acessíveis externamente.

Gráficos e visualizações

- **Configurações incorretas por severidade:** gráfico de barras para crítico, alto, médio e baixo.
- **Achados por categoria:** gráfico de rosca para identidade e acesso (políticas IAM, funções e MFA), rede (grupos de segurança, NACLs, endpoints públicos e VPC), proteção de dados (criptografia e políticas de buckets) e logs e monitoramento (CloudTrail, logs de fluxo, auditoria e alertas).

Recursos principais

- Verificações periódicas de todas as contas conectadas.
- Detecção de lacunas frente a boas práticas e benchmarks.
- Mapeamento dos achados aos benchmarks CIS.
- Reconciliação automática dos achados que deixaram de ser detectados.
- Visão unificada de várias contas e provedores.
- Credenciais criptografadas em repouso.

Primeiros passos

Use [Conectar uma conta](#) para configurar AWS, Azure ou GCP no formulário atual.

O recurso está disponível nos planos empresariais e superiores. O limite de contas depende da licença.

Recursos relacionados

- [Superfície de ataque](#): monitore também os ativos externos.
- [Dashboard](#): indicadores de nuvem no painel principal.

Navegar pelos resultados de nuvem

1. Abra **Segurança em nuvem**.
2. Consulte cartões das contas e informações da última avaliação.
3. Abra uma conta para focar nos recursos e achados.
4. Filtre configurações incorretas por severidade e status.
5. Abra uma linha para revisar recurso, evidências e remediação.

Conectado, **Desconectado** e **Erro** descrevem a conexão. **Nunca avaliado** ou ausência de pontuação indicam que ainda não há resultados, sem significar um ambiente seguro. Consulte [Conectar conta](#) e [Configurações incorretas](#).

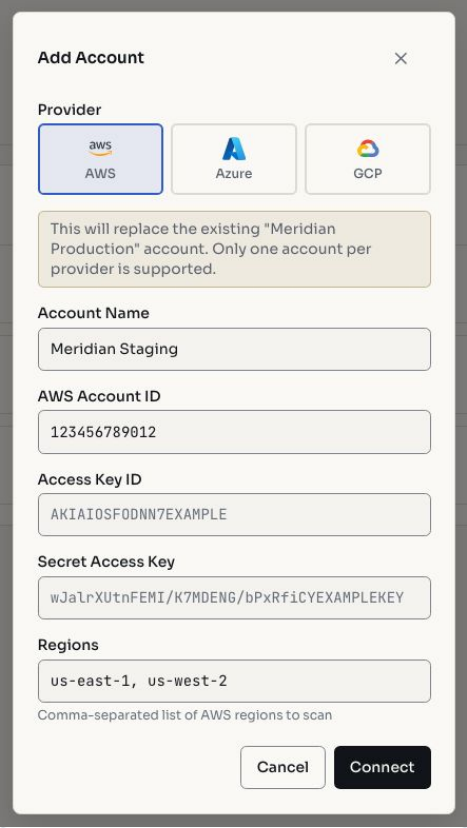
02.08

Conectar uma conta de nuvem

Conecte sua conta AWS, Azure ou GCP para permitir a inspeção da configuração. Você precisa de permissão para gerenciar conexões na organização e criar uma identidade de leitura na conta de nuvem.

Abrir o formulário

1. Abra **Segurança em nuvem**.
2. Use a ação de conexão de conta.
3. Escolha AWS, Azure ou GCP.
4. Informe identificadores e credenciais abaixo.
5. Clique em **Conectar** e confira o resultado.



The screenshot shows a modal window titled "Add Account" with a close button (X) in the top right corner. The form contains the following sections:

- Provider:** Three buttons for "AWS", "Azure", and "GCP". The "AWS" button is selected and highlighted with a blue border.
- Warning:** A yellow box with the text: "This will replace the existing 'Meridian Production' account. Only one account per provider is supported."
- Account Name:** A text input field containing "Meridian Staging".
- AWS Account ID:** A text input field containing "123456789012".
- Access Key ID:** A text input field containing "AKIAIOSFODNN7EXAMPLE".
- Secret Access Key:** A text input field containing "wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY".
- Regions:** A text input field containing "us-east-1, us-west-2". Below this field is the text "Comma-separated list of AWS regions to scan".
- Buttons:** At the bottom right, there are two buttons: "Cancel" and "Connect".

Figura 14 / Conexão de conta de nuvem

Uma conexão válida não significa que a avaliação já terminou. Confira separadamente a data da última avaliação e os resultados.

AWS

O formulário atual recebe:

Campo	Valor
Account ID	Identificador AWS de 12 dígitos
Access Key ID	Chave da identidade de verificação
Secret Access Key	Segredo correspondente
Regiões	Regiões separadas por vírgulas, quando informadas

Crie uma identidade IAM dedicada à inspeção de segurança em leitura. A AWS oferece a política [SecurityAudit](#) para consultar configurações. As permissões exatas dependem dos serviços avaliados; peça ao administrador da nuvem para revisar os requisitos sem conceder escrita irrestrita.

Gere a chave, copie ID e segredo para o formulário e mantenha o segredo no sistema de gestão de credenciais da organização. A interface atual não oferece um assistente de ARN de função. Quando usado, o acesso por função é configurado no fluxo administrativo adequado.

Azure

Crie uma aplicação e uma entidade de serviço no Microsoft Entra ID. Conceda leitura na assinatura, como **Reader** para recursos, com permissões adicionais de segurança apenas quando necessárias. Consulte [Funções internas do Azure](#).

Campo	Valor
Tenant ID	Identificador do diretório
Subscription ID	Assinatura avaliada
Client ID (App ID)	Identificador da aplicação
Client Secret	Valor do segredo, não seu identificador

Registre a expiração e rotacione antes do vencimento. Use a assinatura em que a entidade recebeu acesso.

GCP

Crie uma conta de serviço dedicada no projeto e conceda as permissões de leitura necessárias para recursos e configuração de segurança. Consulte [Funções IAM do Google Cloud](#).

O formulário recebe **Project ID** e a **chave JSON da conta de serviço**. Cole o objeto JSON completo. Se a organização proibir chaves, combine uma configuração aprovada com o administrador. Siga as [orientações de gestão de chaves](#).

Validar e gerenciar

Na lista de contas, abra o menu e use **Validar novamente** após trocar credenciais ou permissões. Confira o estado e a data da validação. O menu também permite remover a conexão conforme a permissão.

Diagnóstico

Sintoma	Verificação
Credenciais inválidas	Identificadores, par de chave e segredo e expiração
Acesso negado	Leitura na conta, assinatura ou projeto correto
Sem resultados	Pode haver conexão antes da primeira avaliação concluída
Falha após rotação	Atualize as credenciais pelo fluxo de gestão disponível
Ação indisponível	Licença e permissões de nuvem

As credenciais são criptografadas em repouso e não retornam nos detalhes comuns da conexão. Não as inclua em descrições de achados, links públicos ou relatórios.

02.09

Configurações incorretas

O Hashiro verifica recursos de nuvem conforme benchmarks e boas práticas. Cada achado representa uma lacuna de segurança ou de conformidade.

Status	Open					Load...
Misconfigurations		All providers		All services	All severiti...	
Severity ↑	Finding	Provider	Resource	Service	CIS Reference	
> Critical	Root account MFA not configured	AWS	root-account	IAM	CIS 6.1	
> High	Unused access keys require rotation	AWS	svc-deployment	IAM	CIS 2.1	
> High	Network rules allow unrestricted SSH	AWS	platform-bastion	EC2	CIS 4.1	
> Medium	Storage bucket lacks access logging	AWS	meridian-audit-archive	S3	CIS 1.1	
> Medium	Database encryption setting needs review	AWS	customer-db-prod	RDS	CIS 3.1	
> Low	Audit trail retention below policy	AWS	organization-trail	CloudTrail	CIS 5.1	

Figura 15 / Tabela de configurações incorretas

Tabela de configurações incorretas

Coluna	Descrição
Título	Descrição do problema
Provedor	AWS, Azure ou GCP
Severidade	Crítico, alto, médio ou baixo
Categoria	IAM, rede, proteção de dados ou logs
Status	Aberto, resolvido ou suprimido
Referência CIS	Controle de benchmark associado
Primeira detecção	Data da identificação inicial

Níveis de severidade

Severidade	Descrição
Crítico	Risco imediato de exposição ou acesso indevido, como buckets públicos com dados sensíveis ou conta root sem MFA
Alto	Lacuna significativa, como grupos de segurança permissivos ou bancos sem criptografia
Médio	Risco moderado, como ausência de logs ou credenciais sem uso
Baixo	Recomendações menores de proteção, como tags e boas práticas não críticas

Categorias

Identidade e acesso (IAM)

Políticas permissivas, conta root sem MFA, chaves antigas ou sem uso, políticas de senha ausentes e acesso entre contas mal configurado.

Rede

Grupos de segurança com entrada 0.0.0.0/0, recursos públicos que deveriam ser privados, falta de segmentação, tráfego sem criptografia e ausência de logs de fluxo VPC.

Proteção de dados

Armazenamento S3, EBS ou RDS sem criptografia, buckets públicos, ausência de criptografia em trânsito, gestão insegura de chaves e backups ausentes.

Logs e monitoramento

CloudTrail ou auditoria desativados, logs de fluxo ausentes, falta de alertas, retenção insuficiente e ausência de logs de acesso a buckets.

Acompanhamento de status

- **Aberto:** problema ativo, ainda sem correção.
- **Resolvido:** correção confirmada manualmente ou pela reconciliação de verificações.
- **Suprimido:** problema reconhecido e intencionalmente mantido, como um risco aceito.

Reconciliação de verificações

Cada nova verificação compara os resultados com os anteriores:

- Novos achados recebem status aberto.
- Achados que deixaram de ser detectados são resolvidos automaticamente, quando o recurso foi corrigido ou removido.
- Achados persistentes mantêm seu status.

Assim, a lista acompanha o estado atual da infraestrutura.

Detalhes da configuração incorreta

Clique em um achado para ver descrição, recurso afetado (ARN ou ID), referência CIS, instruções de remediação e contexto de risco.

Filtros

Filtre por severidade, categoria, provedor e status.

Comece pelos achados críticos de IAM e rede, que representam os riscos mais altos.

Alterar o status

1. Abra **Segurança em nuvem** e localize a tabela.
2. Filtre por status ou severidade.
3. Abra o título do achado para acessar os detalhes.
4. Revise o recurso afetado e a remediação.
5. No seletor próximo ao topo, escolha **Aberto**, **Resolvido** ou **Suprimido**.
6. Confira a confirmação e o novo status. Se houver falha, o seletor volta ao valor anterior e exibe um erro.

Use Resolvido após confirmar a correção. Use Suprimido para achados deliberadamente aceitos ou excluídos. O status não altera o recurso de nuvem. Uma avaliação posterior pode reconciliar o registro conforme as regras da verificação.

Volte à tabela e ajuste o filtro se o achado sair da visualização atual. A edição exige permissões de nuvem da organização; consultar um registro não concede automaticamente acesso para alterar status.

02.10

Conformidade

O Hashiro relaciona configurações incorretas aos benchmarks de segurança para mostrar o alinhamento da infraestrutura aos padrões do setor.

Benchmarks CIS

O principal referencial é o **CIS (Center for Internet Security)**, com diretrizes de boas práticas para ambientes de nuvem.

Provedor	Benchmark
AWS	CIS Amazon Web Services Foundations Benchmark
Azure	CIS Microsoft Azure Foundations Benchmark
GCP	CIS Google Cloud Platform Foundations Benchmark

Pontuação de conformidade

Cada conta conectada mostra o percentual de controles CIS aplicáveis aprovados:

$$\text{Pontuação} = (\text{Controles aprovados} / \text{Total de controles aplicáveis}) \times 100$$

A pontuação é atualizada após cada verificação.

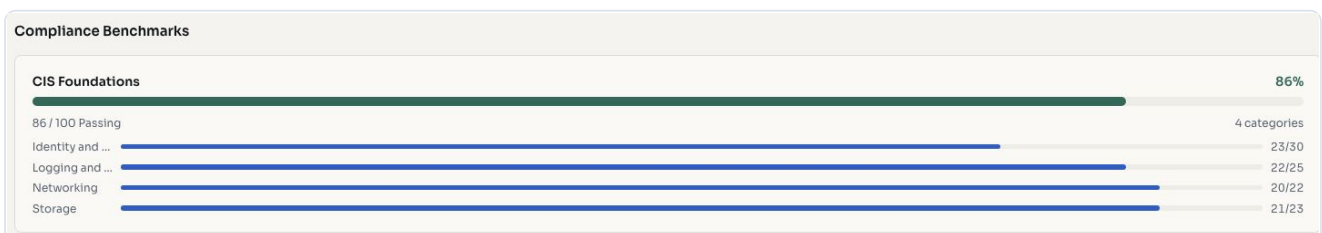


Figura 16 / Pontuação de conformidade e benchmarks

Progresso dos benchmarks

Barras de progresso indicam:

- **Aprovados:** nenhum problema encontrado no controle.
- **Reprovados:** uma ou mais configurações incorretas ativas.
- **Não aplicáveis:** controles sem aplicação no ambiente, como os de serviços não utilizados.

Mapeamento de controles

Cada configuração incorreta é vinculada ao controle CIS correspondente. Abra um controle para ver os achados relacionados ou um achado para ver os controles afetados. Um controle só é aprovado quando todos os problemas relacionados são resolvidos.

Uso dos dados de conformidade

Preparação para auditorias

Exporte relatórios para demonstrar a postura da organização. A visualização mostra controles atendidos, lacunas e recursos envolvidos.

Priorização

Priorize problemas que afetam vários controles ou obrigações regulatórias.

Acompanhamento de tendências

Acompanhe a pontuação ao longo do tempo para verificar melhorias e identificar regressões em novas implantações.

A pontuação é um indicador de boas práticas, mas não substitui uma avaliação completa nem garante ausência de riscos.

02.11

Projetos

Projetos são a unidade central das avaliações de segurança no Hashiro. Cada pentest, programa de bug bounty ou avaliação contínua tem escopo, achados, equipe e entregáveis próprios.

Figura 17 / Portfólio de projetos

Portfólio

Altere entre **lista** e **cartões**. Pesquise pelo nome, filtre por status (ativo, concluído ou arquivado) e navegue pelas páginas. Provedores também filtram por cliente.

Cada cartão mostra achados por severidade, datas, membros e status.

Tipos de projeto

Tipo	Descrição
Caixa-preta	Sem conhecimento prévio do alvo, simulando um atacante externo
Caixa-cinza	Conhecimento parcial, com algumas credenciais ou documentação
Caixa-branca	Acesso completo a código-fonte, arquitetura e credenciais

Recurso de provedores Provedores podem definir tipos de projeto personalizados para seus serviços.

Abas do projeto

Aba	Finalidade
Detalhes	Escopo, credenciais, contexto e configuração
Narrativa	Documentação Markdown da metodologia e do progresso
Ativos	Hosts e subdomínios descobertos
URLs	Caminhos enumerados nos ativos
Serviços	Portas e protocolos identificados
Achados	Vulnerabilidades, severidade, CVSS e status
IA	Avaliações automatizadas

Figura 18 / Abas dos detalhes do projeto

Permissões dos membros

Atribua níveis de acesso específicos por membro dentro do projeto, independentemente da função geral na organização.

Gestão pelo cliente ou provedor

- **Gerenciado pelo provedor:** o provedor controla escopo, achados e relatórios. Clientes podem consultar os resultados e baixar relatórios.

- **Gerenciado pelo cliente:** a organização cliente cria avaliações internas e pode conceder acesso ao provedor para colaboração.

Exclusão de projetos

A exclusão remove ativos, URLs, serviços, achados, insights, execuções de IA, conectores e notificações associados.

A exclusão é irreversível e remove permanentemente os dados associados.

02.12

Gerenciamento de escopo

O escopo define os limites autorizados de uma avaliação e os alvos que não devem ser testados. Ele orienta a descoberta, as verificações e os testes manuais.

Scope and context

ScopeOut of Scope

In Scope

Add Line

Asset	Asset Type	Actions
*.meridian.example.com	domain	 
api.meridian.example.com	domain	 
198.51.100.0/24	cdir	 

Copy to clipboard

Figura 19 / Configuração do escopo

Definir o escopo

Cada projeto tem duas listas:

- **Dentro do escopo:** alvos autorizados.
- **Fora do escopo:** alvos proibidos, mesmo quando encontrados na enumeração.

As entradas são validadas na criação conforme o tipo de ativo.

Tipos de ativo

Tipo	Exemplo	Descrição
Curinga	*.example.com	Todos os subdomínios
Domínio	app.example.com	Hostname específico
IP	192.168.1.1	Endereço individual

Tipo	Exemplo	Descrição
CIDR	10.0.0.0/24	Intervalo de endereços
Aplicativo iOS	com.example.app	Identificador do bundle
Aplicativo Android	com.example.app	Nome do pacote
Código-fonte	github.com/org/repo	Repositório de código

Credenciais e contexto

Inclua contas de teste, chaves de API e material de autenticação para avaliações caixa-cinza ou caixa-branca. Adicione notas Markdown sobre ambiente, arquitetura, tecnologias e orientações de teste.

Contexto detalhado ajuda a equipe e os agentes de IA a entender o ambiente sem uma apresentação separada.

Importar escopo

Importe entradas em lote para avaliações grandes ou para sincronizar um programa de bug bounty.

Escopo e descoberta de ativos

1. Curingas orientam a enumeração de subdomínios.
2. Domínios são consultados para respostas HTTP, tecnologias e serviços.
3. IPs e CIDRs são verificados para identificar portas e serviços.

Os ativos descobertos são validados contra o escopo. Correspondências fora do escopo são sinalizadas e excluídas das verificações automáticas.

02.13

Narrativa

A narrativa é um documento Markdown com metodologia, progresso e contexto geral dos achados. Complementa os dados da aba Achados.

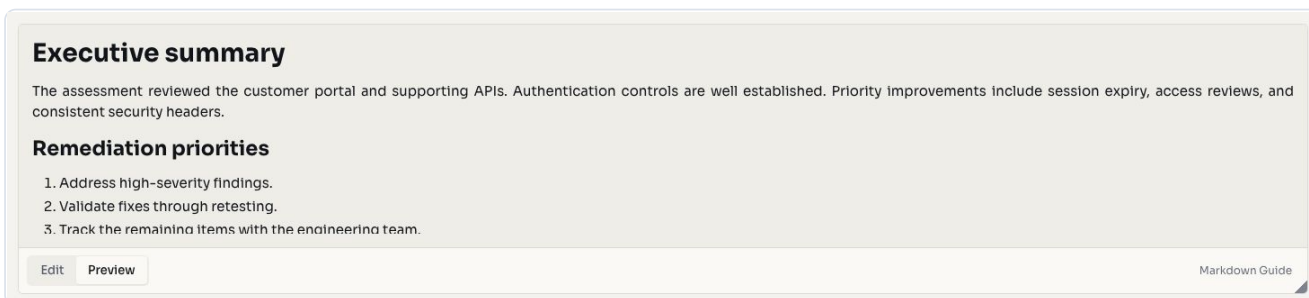


Figura 20 / Editor de narrativa

Escrever a narrativa

O editor aceita títulos, listas, tabelas, blocos de código, imagens e links.

Uma narrativa típica inclui:

- **Resumo executivo:** visão geral para pessoas não técnicas.
- **Metodologia:** ferramentas, etapas e cobertura da avaliação.
- **Visão geral dos achados:** descobertas organizadas por impacto ou categoria.
- **Recomendações:** orientações estratégicas além das correções individuais.

Controle de acesso

Perfil	Acesso
Provedores / Pentesters	Leitura e escrita
Clientes	Somente leitura

Clientes podem consultar a documentação sem modificar o trabalho do provedor.

Narrativa nos relatórios

O conteúdo alimenta o resumo executivo, a metodologia e a descrição geral nos relatórios PDF.

Escreva pensando no relatório final, com linguagem profissional e estrutura adequada ao público.

02.14

Cadeias de ataque

Cadeias de ataque são diagramas que mostram como achados individuais se combinam e ampliam o impacto. Eles ajudam a comunicar o risco agregado.

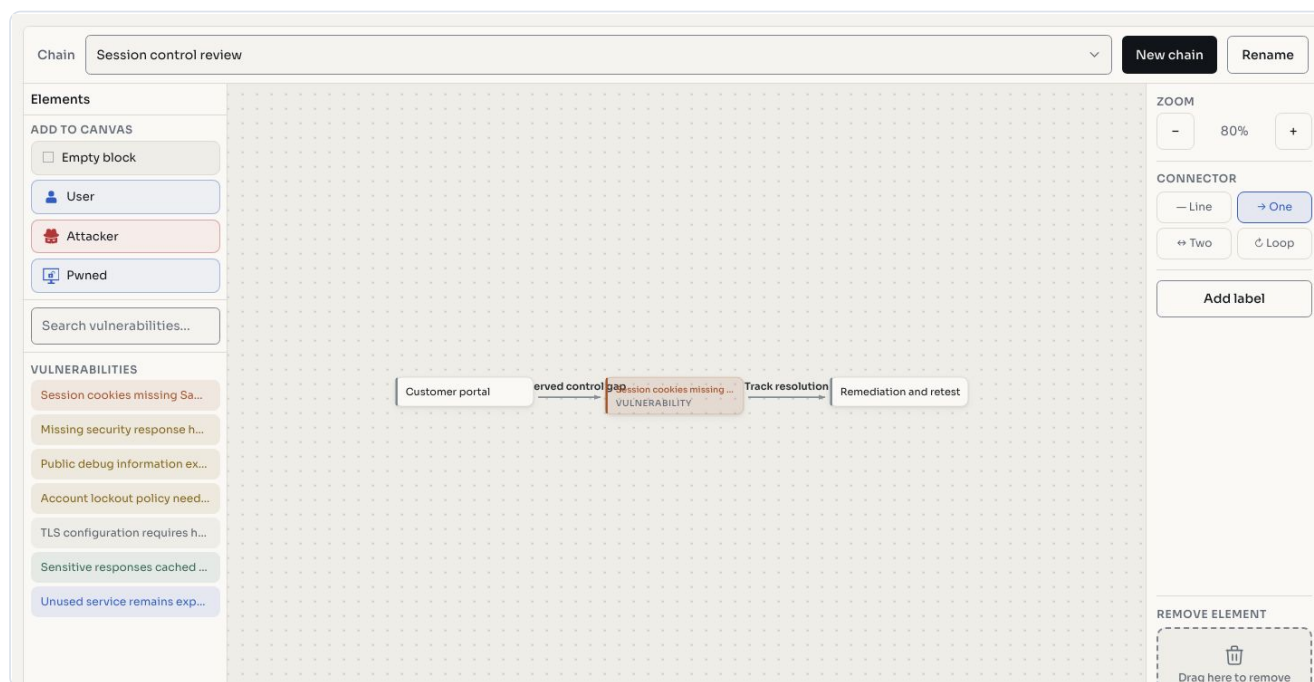


Figura 21 / Editor de cadeias de ataque

Por que usar cadeias

Um achado médio de exposição de informações e uma configuração incorreta baixa podem, juntos, representar um risco crítico. O diagrama torna essa relação visível aos responsáveis.

Tipos de nó

Nó	Finalidade
Vulnerabilidade	Achado existente no projeto
Rótulo	Anotação ou nome de etapa
Bloco	Sistema ou componente, como servidor web ou banco
Pessoa	Função ou identidade de usuário
Atacante	Agente de ameaça inicial
Pwned	Estado final de comprometimento

Construir cadeias

1. Adicione nós para representar as etapas documentadas.
2. Conecte-os com setas direcionais.
3. Vincule os nós de vulnerabilidade aos achados para rastreabilidade.
4. Use rótulos para explicar as transições.

Um projeto pode ter várias cadeias para representar cenários diferentes.

Incluir nos relatórios

Os diagramas são incluídos nos relatórios PDF junto aos achados referenciados, formando uma descrição coerente do risco.

02.15

Geração de relatórios

O Hashiro gera relatórios PDF de pentest a partir da narrativa, escopo, achados, CVSS, cadeias de ataque e orientações de remediação.

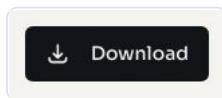


Figura 22 / Download de relatório no projeto

Conteúdo do relatório

- **Capa:** projeto, cliente, datas e classificação.
- **Resumo executivo:** visão geral da narrativa.
- **Escopo:** alvos incluídos e excluídos.
- **Metodologia:** abordagem documentada.
- **Achados:** severidade, CVSS, descrição, evidências e remediação.
- **Cadeias de ataque:** diagramas de riscos combinados.
- **Resumo de remediação:** ações priorizadas.
- **Apêndices:** detalhes técnicos adicionais.

Gerar um relatório

1. Selecione um template e solicite a geração na tela do projeto.
2. Aguarde o processamento do template LaTeX com os dados do projeto.
3. Baixe o PDF quando estiver pronto.

O status pode ser consultado durante o processamento.

Templates

Administradores da plataforma gerenciam templates **LaTeX**, que definem layout, marca, seções e formatação. Uma organização pode ter vários templates, com prévia usando dados de exemplo e acesso concedido por organização.

Solicite ao administrador um template com sua marca, avisos e formatação preferida.

Idiomas

Relatórios podem ser gerados em inglês (en) ou português (pt). O idioma do projeto determina o conteúdo e os títulos das seções.

Armazenamento

Relatórios são armazenados com segurança e podem ser baixados novamente. Gerações anteriores ficam disponíveis até a exclusão do projeto.

02.16

Gestão de vulnerabilidades

A gestão de vulnerabilidades se organiza em **achados**, registros individuais de problemas identificados nas avaliações, desde a descoberta até a remediação.

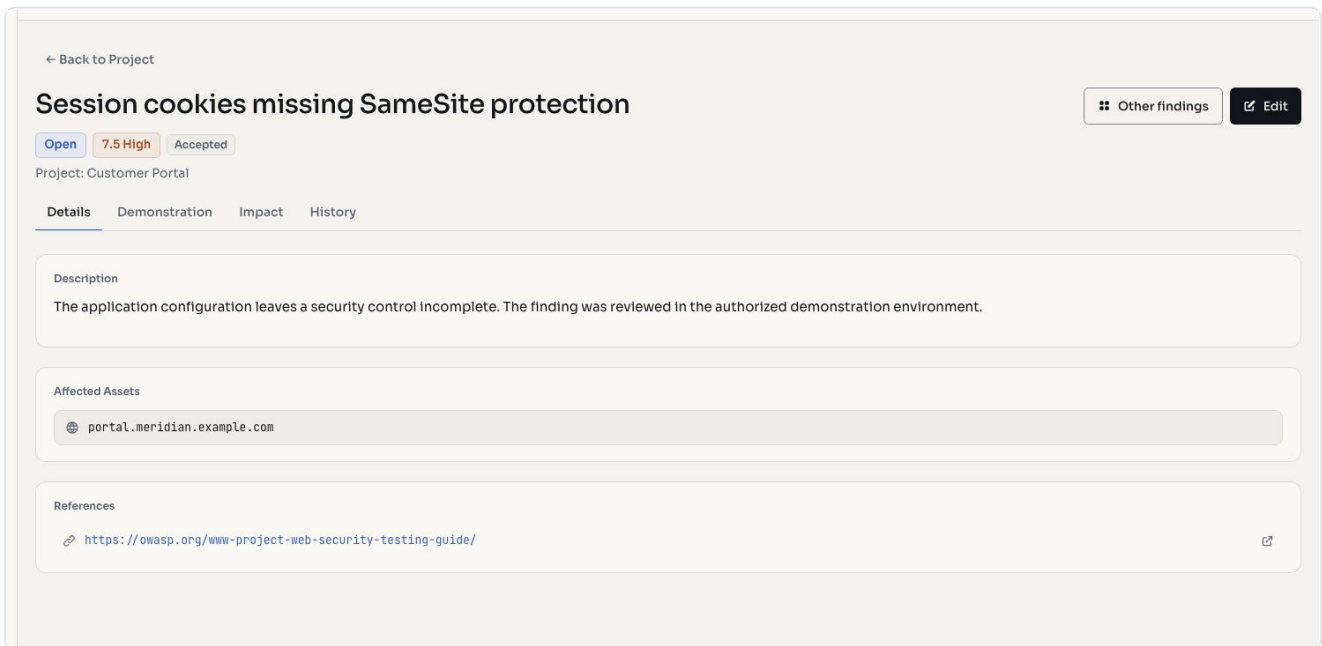


Figura 23 / Detalhes de um achado

Criar achados

Crie manualmente no editor, a partir de templates, de resultados Nuclei ou de candidatos produzidos por avaliações com IA.

Detalhes do achado

Campo	Descrição
Título	Nome claro da vulnerabilidade
Descrição	Explicação detalhada e contexto
Severidade	Crítico, alto, médio, baixo ou informativo
CVSS v3.1	Pontuação padronizada e vetor completo
Status	Estado no ciclo de vida
Ativo	Host, URL ou serviço afetado

Campo	Descrição
Observação	O que foi observado durante os testes
Demonstração	Evidências e passos de validação
Remediação	Correção ou mitigação recomendada
Referências	CVEs, avisos e documentação externa
Evidências	Capturas de tela, dados de teste e respostas

Modo de edição

- **Informações básicas:** título, descrição, severidade, status, ativo e categoria.
- **CVSS / Impacto:** calculadora v3.1 e avaliação de impacto.
- **Informações adicionais:** remediação, referências, observação e demonstração.

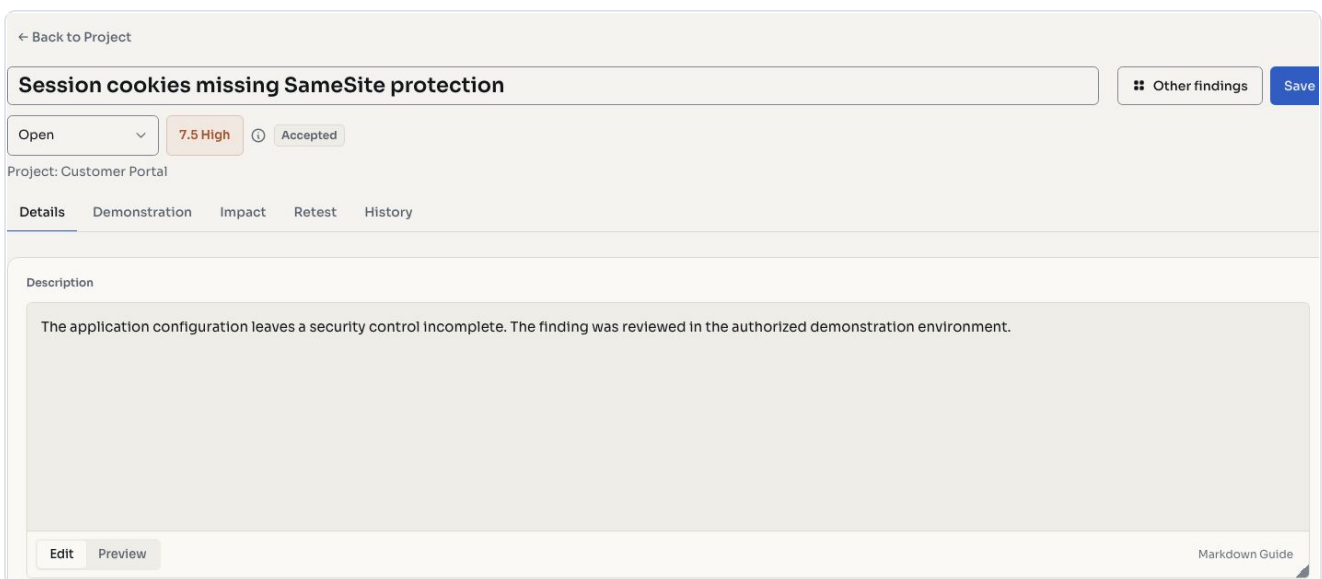


Figura 24 / Abas do editor de achados

Anexos

Envie capturas de tela, registros de requisição e resposta e documentos de apoio como evidências.

Histórico

Cada achado mantém uma **trilha de auditoria imutável** de alterações, transições de status, severidade, retestes e responsáveis.

Navegação

O painel de outros achados permite alternar entre registros do mesmo projeto sem voltar à lista.

Resultados Nuclei

Uma visualização dedicada apresenta resultados paginados, severidade e criação de achados a partir das verificações.

02.17

Ciclo de vida dos achados

Cada achado segue um ciclo estruturado da descoberta à resolução, facilitando o acompanhamento da remediação e a comunicação entre equipes.

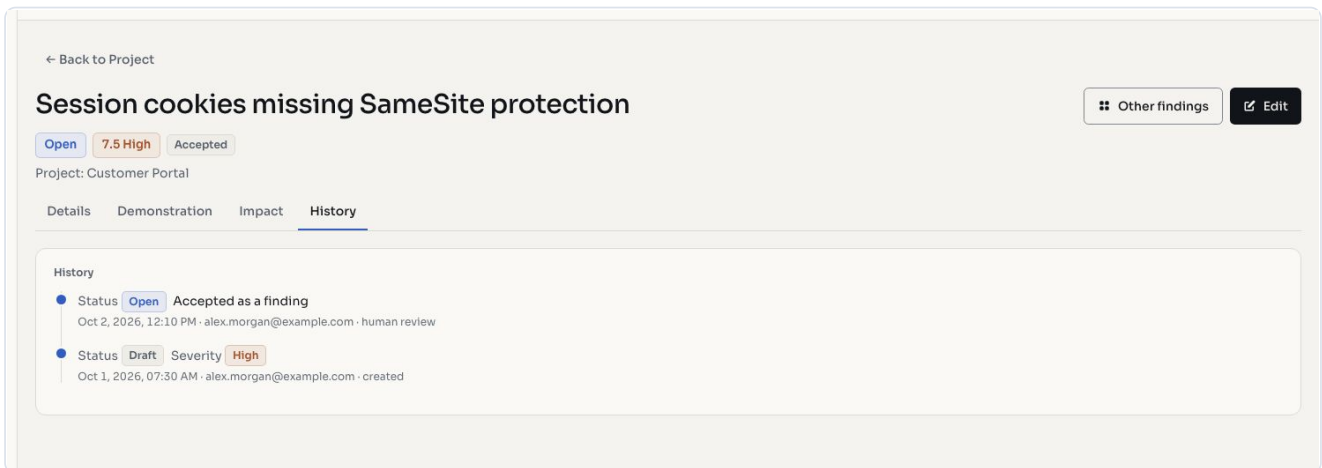


Figura 25 / Fluxo do ciclo de vida

Status

Status	Descrição
Rascunho	Em documentação, ainda invisível aos clientes
Aberto	Vulnerabilidade confirmada e aguardando correção
Fechado	Correção realizada e verificada
Aceito	Risco aceito pelo cliente, sem correção planejada
Reteste pendente	Correção informada pelo cliente, aguardando verificação
Em reteste	Verificação da correção em andamento
Reteste falhou	Correção insuficiente, vulnerabilidade persiste
Não aplicável	Achado não se aplica ao ambiente
Duplicado	Repete outro achado
Informativo	Observação sem impacto direto

Fluxo típico

Rascunho -> Aberto -> Reteste pendente -> Em reteste -> Fechado
-> Reteste falhou -> Aberto

Caminhos alternativos incluem aberto para aceito, não aplicável ou duplicado, e rascunho para informativo.

Verificação de achados de IA

Estado	Significado
Candidato	Aguardando revisão humana
Aceito	Revisor confirmou a validade
Rejeitado	Revisor considerou inválido
Precisa de evidência	Provas adicionais solicitadas
Mesclado	Combinado com outro achado

Candidatos podem ficar **visíveis aos clientes** antes da verificação completa, enquanto o provedor revisa a precisão dos resultados.

Acompanhamento de retestes

1. O cliente informa uma correção e o achado passa a **reteste pendente**.
2. O pentester inicia a verificação e muda para **em reteste**.
3. O resultado é **fechado**, se a correção funcionou, ou **reteste falhou**, se o problema persiste.

Comentários registram os testes e resultados de cada tentativa.

Operações em lote

Selecione vários achados para alterar status ou excluí-los.

As operações afetam todos os registros selecionados imediatamente. Confira a seleção antes de aplicar.

Trilha de auditoria

O histórico imutável registra o que mudou, quem realizou a alteração e quando, incluindo status, severidade e retestes.

02.18

Pontuação CVSS

O Hashiro usa o **Common Vulnerability Scoring System v3.1** para padronizar a severidade e comunicar o risco dos achados.

CVSS 3.1 Score Calculator

Attack Vector (AV)

Network (N)

Adjacent (A)

Local (L)

Physical (P)

Attack Complexity (AC)

Low (L)

High (H)

Privileges Required (PR)

None (N)

Low (L)

High (H)

User Interaction (UI)

None (N)

Required (R)

Scope (S)

Unchanged (U)

Changed (C)

Confidentiality (C)

None (N)

Low (L)

High (H)

Integrity (I)

None (N)

Low (L)

High (H)

Availability (A)

None (N)

Low (L)

High (H)

Score

7.5

High

CVSS 3.1 Vector String

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Figura 26 / Calculadora CVSS

Calculadora de pontuação

Configure os componentes do vetor. O resultado é calculado automaticamente.

Métricas de explorabilidade

Métrica	Valores	Descrição
Vetor de ataque (AV)	Rede, adjacente, local, físico	Meio de exploração
Complexidade (AC)	Baixa, alta	Condições fora do controle do atacante
Privilégios necessários (PR)	Nenhum, baixos, altos	Acesso prévio necessário
Interação do usuário (UI)	Nenhuma, necessária	Necessidade de ação de um usuário

Escopo

Métrica	Valores	Descrição
Escopo (S)	Inalterado, alterado	Impacto além do componente vulnerável

Métricas de impacto

Métrica	Valores	Descrição
Confidencialidade (C)	Nenhum, baixo, alto	Exposição de informações
Integridade (I)	Nenhum, baixo, alto	Alteração de dados
Disponibilidade (A)	Nenhum, baixo, alto	Disponibilidade do serviço

Classificação de severidade

Pontuação	Severidade
9,0 a 10,0	Crítico
7,0 a 8,9	Alto
4,0 a 6,9	Médio
0,1 a 3,9	Baixo
0,0	Informativo

Vetor

O vetor codifica as métricas em um formato compacto, armazenado com o achado e incluído nos relatórios:

```
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
```

Uso no Hashiro

A pontuação orienta a priorização nos projetos, aparece nos relatórios PDF e nos indicadores de severidade do dashboard. A matriz de esforço combina severidade e complexidade de remediação.

02.19

Revisão assistida por IA

Avaliações com IA produzem **candidatos**, rascunhos de achados que precisam de revisão humana antes da finalização. O fluxo ajuda a triar, validar e refinar os resultados.

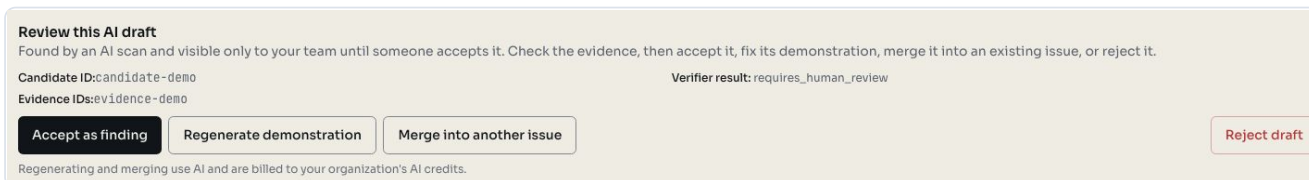


Figura 27 / Painel de revisão de candidatos

Painel de candidatos

Na aba Achados do projeto, cada candidato permite:

Ação	Efeito
Aceitar	Confirma o achado e cria um registro completo
Rejeitar	Descarta falso positivo ou resultado irrelevante
Precisa de evidência	Solicita provas adicionais
Mesclar	Combina com um achado existente da mesma vulnerabilidade

Candidatos podem ficar visíveis aos clientes antes da verificação, enquanto o provedor conclui a revisão.

Regenerar a demonstração

1. Selecione um achado aceito ou em andamento e solicite a regeneração.
2. A IA atualiza a documentação de validação.
3. Revise a prévia.
4. Aplique o conteúdo ou descarte-o.

Use esse recurso para melhorar clareza, formatação ou contexto das evidências.

Propostas de mesclagem

A IA analisa semelhanças e propõe combinar achados sobrepostos. Revise os registros envolvidos e aceite ou rejeite. A aceitação produz um achado consolidado, reduzindo duplicações nos relatórios.

Integração com o fluxo

A revisão segue o [ciclo de vida](#):

```
Avaliação com IA -> Candidato -> Revisão -> Aceito (achado aberto)
                                     -> Rejeitado (arquivado)
                                     -> Mesclado (com registro existente)
```

Todas as ações ficam no histórico do achado.

02.20

Avaliações com IA

Uma avaliação com IA organiza a revisão de segurança dentro de um projeto. Uma **execução de IA**, ou **AI run**, representa uma execução dessa avaliação: possui perfil, escopo, modo, orçamento, progresso e resultados próprios. Um projeto pode reunir várias execuções para comparar observações, revisar mudanças e acompanhar correções ao longo do tempo.

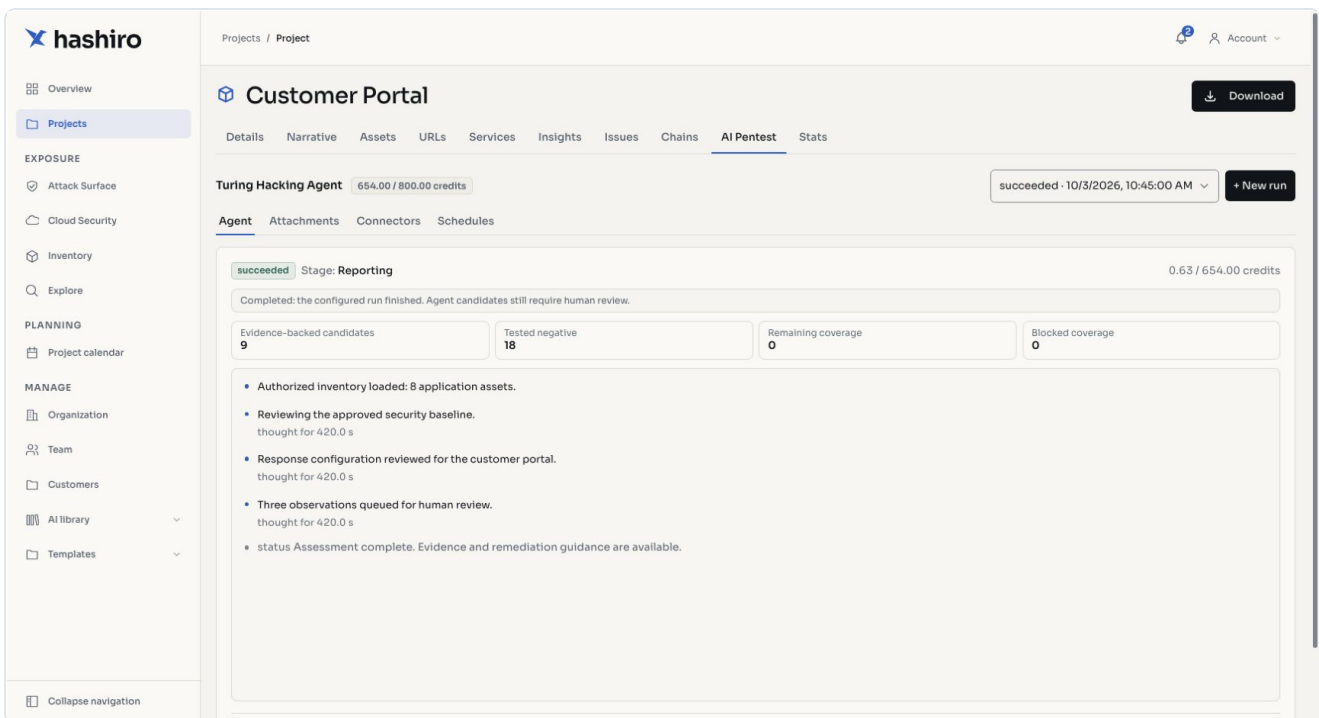


Figura 28 / Área de avaliações com IA

Entenda os tipos de execução

Quatro escolhas descrevem aspectos diferentes de uma execução. Selecionar uma delas não determina automaticamente as outras.

Escolha	O que determina	Exemplos
Modo de interação	Como o operador participa	Automático, Assistido, Checklist
Intenção da avaliação	Abrangência e profundidade da revisão	Lightweight, Balanced, Deep, Continuous
Local de execução	Como a avaliação acessa o ambiente	Acesso gerenciado pela plataforma, acesso local ou à rede privada
Finalidade da avaliação	Qual resultado a equipe quer avaliar	Achados de segurança, revisão de correções, validação purple team por um plugin

[Execuções de IA](#) explica essas escolhas, os requisitos, os orçamentos, o progresso, os resultados e a revisão em detalhes. [Modos de execução](#) apresenta os controles e como iniciar uma avaliação.

Automático, Assistido e Checklist

O modo **Automático** segue o perfil configurado sem interação contínua pelo chat. O modo **Assistido** permite que um operador do provedor oriente a revisão pelo chat. O modo **Checklist** organiza o trabalho em torno de uma lista selecionada e registra a cobertura dos itens. A disponibilidade depende da organização, das permissões no projeto e dos perfis e checklists configurados.

Clientes normalmente usam execuções automáticas quando o provedor habilita essa opção no projeto. Os controles de provedores e clientes podem ser diferentes. Consulte [Avaliações automáticas](#) e [Execuções de IA](#).

Execuções locais

Um ambiente privado pode exigir acesso local por um conector do projeto. Essa escolha descreve a conectividade ao ambiente, e não outro modo de interação. A conexão do relay e a autorização do escopo são requisitos distintos. Consulte [Execuções locais](#) para entender prontidão, responsabilidades e interpretação dos resultados.

Execuções purple team por um plugin

Quando habilitado para a organização, um plugin pode oferecer validação coordenada de controles defensivos. A equipe verifica se a atividade prevista ocorreu, se a telemetria relevante estava disponível e se a detecção e a resposta funcionaram conforme o esperado. Consulte [Execuções purple team](#) para conhecer finalidade, papéis, categorias de resultado e processo de revisão.

Revise os resultados

O progresso e as observações geradas não substituem a revisão humana. Uma execução concluída pode conter candidatos, cobertura incompleta ou trabalho bloqueado. Revise as evidências, aceite ou rejeite candidatos, mescle duplicações quando necessário e acompanhe os achados aceitos pelo fluxo de issues do projeto.

Configurações relacionadas

Tópico	Finalidade
Tipos de agente	Perfis disponíveis para a categoria do projeto
Checklists	Objetivos repetíveis e cobertura dos itens
Conectores	Conectividade com ambientes privados
Base de conhecimento	Referências e contexto do trabalho
Créditos e cobrança	Saldo disponível e gestão de orçamento

Tópico	Finalidade
Agendamentos	Avaliações recorrentes quando disponíveis

02.21

Execuções de IA

Uma **execução de IA**, ou **AI run**, é uma execução de avaliação associada a um projeto. Ela registra a configuração utilizada, o progresso e os resultados. O projeto reúne o trabalho mais amplo, o escopo incluído, as exclusões, o acesso da equipe e o histórico dos achados.

Use execuções separadas quando o objetivo mudar ou quando uma correção exigir nova revisão. Uma execução anterior preserva evidências do que foi revisado naquele momento; ela não comprova o estado atual de uma aplicação que mudou desde então.

Escolha o tipo adequado

Não confunda modo de interação, intenção da avaliação e local de execução. Uma execução automática pode usar a intenção Balanced e um conector para acessar um ambiente privado. Um checklist pode organizar a revisão desse mesmo ambiente. A validação purple team por um plugin tem uma finalidade diferente da descoberta de achados em aplicações.

Objetivo	Escolha relevante	O que revisar depois
Conduzir uma avaliação configurada com revisão periódica do operador	Automático	Evidências, candidatos e trabalho incompleto
Manter um operador envolvido durante a revisão	Assistido	Decisões do operador, observações e achados resultantes
Seguir um conjunto repetível de objetivos de revisão	Checklist	Resultado e evidências de cada item
Revisar um ambiente que exige acesso à rede local	Acesso local ou à rede privada	Conectividade, escopo e resultados da avaliação
Avaliar detecção e resposta em um exercício coordenado	Purple team por um plugin	Evidências de execução, telemetria, detecções e resposta

Modos de interação

Automático

A execução segue o perfil configurado sem interação contínua pelo chat. O operador continua responsável por definir o contexto, acompanhar o progresso e avaliar os candidatos. Automático significa que a revisão configurada pode prosseguir sem acompanhamento contínuo; não significa cobertura ilimitada, achados garantidos ou aceitação automática de todas as observações.

Use esse modo para uma revisão de referência definida, uma avaliação repetida ou um trabalho com escopo e orçamento estabelecidos. Verifique requisitos e saldo antes de iniciar. Consulte [Avaliações automáticas](#).

Assistido

Um operador do provedor orienta a avaliação pelo chat. Esse modo é útil quando a revisão exige interpretação do comportamento da aplicação, esclarecimento de contexto ou decisões sobre quais observações precisam de revisão adicional.

Mantenha as orientações dentro do escopo e das permissões existentes. O chat não amplia o acesso ao projeto. Um operador pode assumir uma execução automática ativa quando o controle correspondente estiver disponível. A disponibilidade difere entre contas de provedores e clientes.

Checklist

A execução segue um checklist disponível, em vez de depender apenas de um objetivo amplo. O checklist expressa o que deve ser revisado e facilita a comparação da cobertura entre execuções.

Um checklist curado agrupa itens específicos em conjuntos. Um template de cobertura organiza a revisão por categorias. Leia o resultado de cada item junto com suas evidências: revisão sem achado, achado identificado, item não aplicável e trabalho bloqueado têm significados diferentes. Um item não revisado não deve ser interpretado como um controle aprovado.

O seletor aparece somente quando existe um checklist apropriado. O checklist organiza evidências, mas não comprova, sozinho, conformidade com uma norma inteira.



Figura 29 / Modos de interação disponíveis

Intenção da avaliação

A intenção descreve o nível de aprofundamento da revisão configurada. É uma escolha separada de Automático ou Checklist. Execuções assistidas seguem a orientação do operador e não apresentam esse seletor de profundidade.

Intenção	Ênfase prevista	Consideração de planejamento
Lightweight	Revisão inicial mais restrita	Útil com tempo ou créditos limitados; espere menor cobertura.
Balanced	Revisão delimitada das áreas mais relevantes	Revise a cobertura e as áreas bloqueadas antes de decidir se mais trabalho é necessário.
Deep	Revisão mais detalhada do ambiente configurado	Reserve mais tempo e créditos; maior esforço não garante cobertura completa.

Intenção	Ênfase prevista	Consideração de planejamento
Continuous	Ciclos repetidos dentro dos limites configurados	Defina um orçamento deliberado e acompanhe mudanças, cobertura e consumo.

Continuous não é um agendamento recorrente. Um agendamento cria execuções separadas nos horários configurados; Continuous se aplica ao trabalho dentro de uma execução. Nenhuma dessas opções elimina a revisão dos resultados.

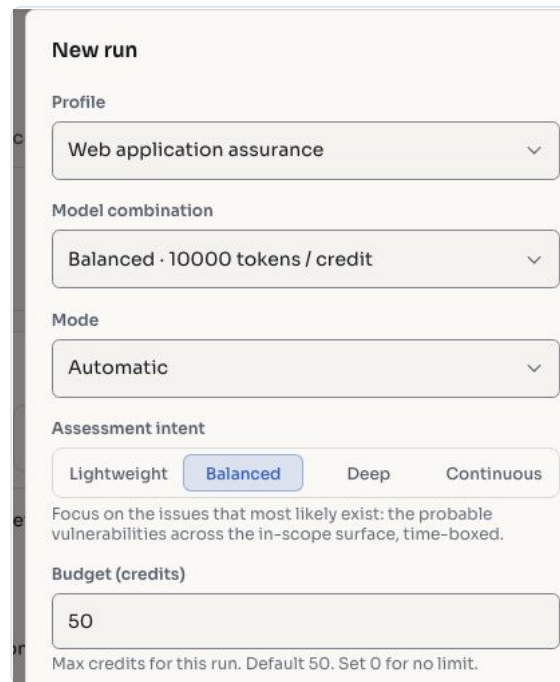


Figura 30 / Configuração de perfil, intenção e orçamento

Perfis e combinações de modelos

Um perfil define as etapas e os objetivos da avaliação configurada. A categoria do projeto e as configurações da organização determinam quais perfis são oferecidos. Escolha um perfil adequado ao ambiente e à finalidade do trabalho.

Uma combinação de modelos, quando oferecida, seleciona a configuração de IA disponível para aquela execução. Ela pode afetar o consumo de créditos e a forma de processamento do perfil. Uma configuração mais cara não garante mais achados válidos. Compare os resultados pelas evidências e pela cobertura, e não apenas pelo custo.

Escopo, acesso e requisitos

Antes de criar uma execução, revise escopo incluído, exclusões, permissões, contexto relevante e créditos. Sem escopo incluído, a avaliação não executa. Um perfil disponível não inclui automaticamente qualquer alvo no trabalho.

Para clientes, o projeto precisa permitir execuções de IA pelo cliente. Para provedores, confirme que o projeto selecionado corresponde ao trabalho autorizado correto. Se o ambiente exigir conectividade

com uma rede privada, consulte [Execuções locais](#). Se exigir um plugin, verifique se a organização possui a funcionalidade habilitada.

Orçamentos e interrupção

O orçamento de créditos delimita os recursos disponíveis para a execução. O valor **0** significa ausência de um teto explícito de créditos por execução no formulário; não significa uso gratuito. O saldo da organização e outros limites aplicáveis continuam relevantes.

Uma execução pode terminar antes de concluir todo o trabalho previsto por causa do orçamento, de uma ação do operador, de um requisito ausente ou de um erro. Revise o status final e o trabalho já registrado. A interrupção preserva observações e achados existentes; ela não certifica o escopo restante.

Acompanhe o progresso

Use o seletor para abrir a execução desejada. Confira status, etapa atual, consumo de créditos, observações e cobertura. O histórico de uma execução concluída permanece separado de uma execução mais recente.

Diferencie espera por requisitos, trabalho ativo, conclusão, cancelamento e falha. Problemas de conectividade ou requisitos ausentes exigem investigação da configuração; não comprovam que o ambiente está livre de problemas de segurança.

Para conhecer os controles e o procedimento de início, consulte [Modos de execução](#).

Interprete o resultado

Resultado	O que informa	O que não informa
Candidato a achado	Uma observação precisa de revisão das evidências	Que o problema já foi aceito ou verificado por uma pessoa
Achado aceito	Um revisor aceitou o problema no fluxo do projeto	Que a correção foi concluída
Revisão sem achado	A revisão registrada não estabeleceu um problema	Que todos os problemas possíveis foram descartados
Cobertura bloqueada ou incompleta	Parte da revisão prevista não pôde ser concluída	Que a área afetada foi aprovada
Execução concluída	O processamento terminou	Que todos os candidatos são válidos ou que a cobertura é completa

Revise evidências, contexto e ativos afetados antes de decidir. Aceite candidatos válidos, rejeite os que não têm suporte ou mescle duplicações quando apropriado. Mantenha o resultado da execução separado do status dos achados: a execução pode estar concluída enquanto seus achados aceitos continuam abertos.

Repita avaliações e compare execuções

Registre o que mudou: escopo, versão do ambiente, perfil, checklist, intenção, orçamento e condições de acesso. Compare cobertura e evidências junto com a quantidade de achados. Menos achados podem representar correções, escopo diferente, trabalho incompleto ou acesso diferente.

Para acompanhar correções, revise o achado afetado e use o fluxo de reteste do projeto. Uma nova execução pode fornecer observações adicionais, mas sua conclusão não deve fechar um achado automaticamente.

Responsabilidades de provedores e clientes

Provedores disponibilizam perfis e permissões adequados, coordenam o acesso ao ambiente e revisam os objetivos. Clientes revisam seu projeto autorizado, créditos disponíveis, resultados e correções. Os botões exibidos para cada conta podem ser diferentes.

Se um perfil, checklist, opção de acesso local ou funcionalidade de plugin estiver ausente, peça ao provedor ou administrador para verificar a disponibilidade. Não substitua o método de execução sem revisar os requisitos do trabalho.

02.22

Execuções locais

O acesso local é relevante quando a avaliação precisa revisar um ambiente acessível apenas por uma máquina autorizada ou rede privada. No fluxo documentado do projeto, um **conector** permite acessar esse ambiente enquanto a avaliação permanece associada ao projeto no Hashiro.

O acesso local descreve o local e a conectividade da execução. Não é um quarto modo de interação: a execução ainda pode usar Automático, Assistido ou Checklist, conforme a disponibilidade.

Acesso local e execução local são diferentes

Conceito	Significado
Acesso à rede privada	A avaliação acessa um ambiente privado autorizado por um conector conectado ao projeto.
Execução totalmente local	O próprio mecanismo de avaliação roda na máquina do operador ou no ambiente local. Isso exige uma opção de execução com suporte específico.
Execução por plugin	Um plugin oferece uma capacidade de avaliação, como validação purple team, quando habilitado para a organização.

Selecionar um conector não comprova que toda a avaliação roda na sua máquina. Também não comprova processamento offline nem que os resultados nunca saem do ambiente. Confira com o provedor as configurações da organização e os requisitos de tratamento dos dados.

Quando o acesso local é útil

Exemplos incluem aplicações privadas, uma API interna, um ambiente de homologação acessível apenas por uma rede aprovada ou um ambiente com requisitos específicos de acesso. A conectividade é apenas um requisito: o projeto também precisa conter o escopo incluído e as exclusões corretas.

Uma máquina acessível por um conector não inclui automaticamente na avaliação todos os recursos que essa máquina consegue acessar.

Responsabilidades antes da execução

O provedor e o responsável pelo ambiente devem acordar o ambiente pretendido, o acesso autorizado, o objetivo da revisão, a janela de trabalho e o tratamento das evidências. Mantenha o contexto do projeto atualizado para permitir a interpretação das observações.

O operador deve confirmar que o projeto oferece o conector necessário, que ele corresponde ao ambiente correto e que seu status é conectado. Use as instruções de configuração fornecidas pela organização e revise o acesso com o responsável pelo ambiente. Instalação e configuração dependem do ambiente e não devem ser deduzidas de uma captura genérica.

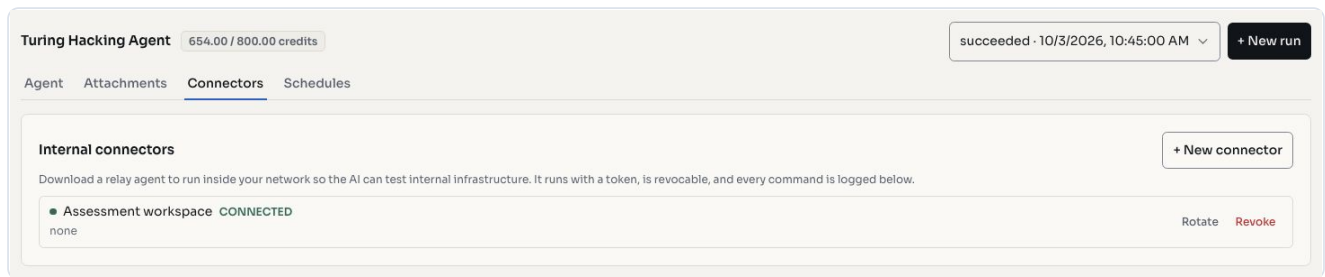


Figura 31 / Status do conector do projeto

Prontidão no projeto

Abra **AI Pentest** no projeto e revise o painel de conectores. O status conectado indica que o relay está disponível; não comprova que todas as aplicações pretendidas estão acessíveis nem que todos os requisitos foram satisfeitos.

Revise a prontidão em três partes:

Parte	O que confirmar
Projeto	Trabalho correto, escopo incluído, exclusões e permissões
Ambiente	Acesso adequado aos recursos privados pretendidos e contexto necessário
Execução	Perfil, modo, intenção, orçamento e conector adequados

Se houver mais de um conector, identifique qual ambiente cada um representa antes de escolher. Não selecione um conector apenas porque está conectado.

Acompanhe o acesso separadamente dos resultados

Acompanhe status e informações de última atividade do conector junto com o progresso da execução. Os registros de atividade disponíveis ajudam a diferenciar um problema de acesso de uma observação da avaliação.

Se a conexão cair, parte da revisão pode ficar bloqueada ou incompleta. Restaure o acesso aprovado pelo processo normal de suporte do ambiente e revise a cobertura afetada antes de decidir por uma nova execução. Áreas não revisadas não devem ser consideradas aprovadas porque a execução terminou sem registrar problemas.

Um conector conectado não garante sucesso. Contexto ausente, dependências indisponíveis, créditos insuficientes e erros de execução também podem afetar o resultado.

Revise e encerre o trabalho

Revise candidatos e evidências pelo projeto, usando o mesmo fluxo de achados das outras execuções de IA. Separe o histórico de atividade do conector da aceitação de um achado: atividade demonstra que houve trabalho, enquanto um achado exige evidência do problema.

Ao concluir, peça ao responsável pelo ambiente para revisar se o acesso local continua necessário. Revogação e rotação de conectores fazem parte da gestão autorizada de acesso. Preserve as evidências conforme os requisitos de retenção da organização.

Para os modos de operação, consulte [Execuções de IA](#). Para um exercício defensivo coordenado com um plugin, consulte [Execuções purple team](#).

02.23

Execuções purple team

Uma execução purple team é um exercício coordenado que avalia visibilidade defensiva e resposta em relação a um objetivo de validação acordado. Quando habilitado para a organização, um **plugin** fornece essa capacidade de avaliação. A disponibilidade depende do acesso da organização e da configuração do plugin; ela não acompanha automaticamente toda avaliação de IA.

A finalidade é entender a relação entre atividade observada, telemetria, detecções e resposta. Um achado em uma aplicação e uma lacuna de detecção são resultados diferentes e devem ser revisados separadamente.

Compare as finalidades

Aspecto	Avaliação de segurança com IA	Execução purple team por um plugin
Pergunta principal	Quais observações de segurança com suporte devem ser revisadas?	Os controles defensivos observaram e responderam à validação acordada?
Contexto típico	Escopo do projeto, contexto da aplicação, perfil e objetivos de cobertura	Objetivo de validação, ambiente, telemetria disponível e expectativas defensivas
Evidências	Observações que sustentam candidatos e revisão de correções	Registros de execução, telemetria, detecções e resposta
Acompanhamento	Aceitar ou rejeitar candidatos e acompanhar correções	Investigar lacunas de detecção ou resposta e verificar melhorias

Um exercício purple team não substitui uma avaliação de aplicação. A avaliação da aplicação também não comprova que o monitoramento e a resposta detectariam o comportamento avaliado em um exercício purple team.

Papéis e coordenação

O **provedor ou coordenador** define o objetivo autorizado, confirma a disponibilidade da funcionalidade e coordena o exercício com o responsável pelo ambiente. O **responsável pelo ambiente** confirma ambiente aprovado, janela de trabalho e requisitos de acesso. A **equipe defensiva** identifica a telemetria relevante e os resultados esperados de detecção e resposta.

O **revisor** concilia os registros da execução com as evidências da equipe defensiva. Em equipes menores, as mesmas pessoas podem exercer vários papéis, mas as responsabilidades continuam distintas.

A visibilidade de provedores e clientes pode diferir. Um cliente deve visualizar apenas as opções e os resultados disponibilizados para sua organização. A administração do plugin e a configuração do acesso ficam com os administradores autorizados.

Defina o objetivo antes da execução

Registre a pergunta defensiva que deseja responder. Exemplos incluem verificar se um controle produz a telemetria esperada, se um alerta chega à equipe responsável ou se o processo de resposta registra o acompanhamento previsto.

Documente o ambiente e os critérios de sucesso para permitir a avaliação do resultado. Um registro útil inclui objetivo, ambiente permitido, fontes de evidência esperadas, janela relevante, revisores responsáveis e condições que tornariam o resultado inconclusivo.

Não trate toda execução bem-sucedida como uma validação defensiva bem-sucedida. A execução pode terminar sem a telemetria necessária para avaliar o objetivo.

Tipos de execução e profundidade

Purple team descreve a finalidade do exercício. Não deve ser confundido com Automático, Assistido ou Checklist no formulário de IA. Um plugin pode apresentar controles e requisitos diferentes dos de uma execução comum de IA.

Uma validação focada responde a uma pergunta defensiva mais restrita. Um exercício mais amplo pode revisar vários objetivos, mas cada objetivo exige evidências e resultado próprios. Uma repetição verifica uma melhoria em relação à referência anterior. Agendamentos, quando oferecidos, criam outra execução e não eliminam a coordenação da revisão.

Use somente as opções efetivamente disponibilizadas pelo plugin para a organização. A existência de um perfil de IA não implica suporte pelo plugin, e um item de catálogo não implica que os requisitos de execução estejam prontos.

Disponibilidade e prontidão

A organização precisa da funcionalidade habilitada, de uma opção de validação disponível, das permissões necessárias e de um ambiente que satisfaça os requisitos do plugin. Quando houver um componente local, o responsável deve seguir as instruções fornecidas para aquele ambiente específico.

O conector documentado de IA e o componente local de um plugin são conceitos separados. Não presuma que um substitui o outro. Consulte [Execuções locais](#) para distinguir acesso à rede privada e execução local.

Se não houver uma opção compatível, peça ao provedor para revisar acesso e configuração. Problemas de conexão, requisitos ausentes ou telemetria indisponível devem permanecer registrados como resultados incompletos ou inconclusivos, em vez de serem considerados aprovação do controle.

Acompanhe e reúna as evidências

Mantenha o status de execução separado do resultado defensivo. Revise se a validação pretendida ocorreu, se o ambiente estava pronto durante o período relevante e se as evidências necessárias estão disponíveis.

Quando o plugin apresentar histórico ou artefatos, use esses registros junto com a telemetria e os registros de incidentes da equipe defensiva. Correlacione ambiente e janela de tempo. Um registro de execução, sozinho, não comprova que um alerta foi gerado, entregue, investigado ou resolvido.

Interprete os resultados separadamente

Categoria	Pergunta para o revisor
Execução	A validação acordada ocorreu ou ficou bloqueada ou incompleta?
Telemetria	A observação esperada foi registrada e está disponível para revisão?
Deteção	O controle previsto produziu a deteção esperada?
Resposta	A investigação ou resposta prevista foi realizada e registrada?

Essas categorias podem apresentar resultados diferentes na mesma execução. A atividade pode ocorrer sem a deteção esperada. Uma deteção pode ocorrer sem uma resposta concluída. A ausência de telemetria pode impedir uma conclusão mesmo quando a execução terminou.

Use resultados claros, como sustentado por evidências, não sustentado, bloqueado e inconclusivo. Preserve as evidências e explique a conclusão do revisor. Não afirme um nível de proteção mais amplo do que o exercício comprovou.

Achados e correções

Uma lacuna defensiva deve identificar o controle revisado, o resultado esperado, a observação real, as evidências e a equipe responsável pelo acompanhamento. Ela pode exigir mudanças de configuração, melhorias de telemetria, revisão de alertas ou correção de processos.

Acompanhe o trabalho aceito pelo processo de issues da organização quando esse fluxo estiver disponível. Mantenha o status dos achados separado do status da execução. Uma execução purple team concluída não significa que suas ações de acompanhamento foram encerradas.

Após as melhorias, compare a nova validação com o objetivo e as evidências originais. Registre mudanças no ambiente ou nas condições de validação para preservar o significado da comparação.

Para modos de interação e revisão dos resultados, consulte [Execuções de IA](#) e [Modos de execução](#).

02.24

Tipos de agente

Tipos de agente são definições reutilizáveis de avaliação, com etapas, ferramentas, modelos e capacidades.

Edit profile [X]

Basics

Name
Web application assurance

Description
Review application security controls and organize evidence for human review.

Directions
Review the approved inventory and document security control observations for human review.

Always-on brief for this agent: what it's for and how it should operate. Applied to every stage. 90 / 8192

Main AI license
Select a license [v]

Default model
Medium [v]

Orchestrates the run; stages can override it below. Resolved by the run's chosen model combination.

Figura 32 / Editor de tipos de agente

Criar um tipo de agente

Etapas

Cada definição contém uma ou mais etapas sequenciais:

Campo	Descrição
Objetivo	Resultado esperado da etapa
Prompt de sistema	Instruções de comportamento
Ferramentas	Recursos disponíveis, como consultas HTTP, Galileo e base de conhecimento
Classes de operação	Categorias de ações permitidas
Limites de efeito	Restrições sobre ações destrutivas ou de alto impacto
Orçamento de tokens	Consumo máximo de tokens

Campo	Descrição
Ciclos	Limite de ciclos de execução

Um fluxo típico contém descoberta, análise, validação e relatório.

Pacotes de capacidades

Bundles agrupam ferramentas e permissões relacionadas para compor capacidades sem configurar cada item separadamente.

Licença de IA

Cada tipo é associado a uma licença que determina o provedor LLM e a credencial utilizada.

Seleção de modelos

Configure o modelo de **execução** e, opcionalmente, o **estrategista**. Combinações por nível adaptam a capacidade do modelo à complexidade da tarefa.

Recursos avançados

Cobertura ampla

Uma avaliação geral em segundo plano pode complementar a análise principal, ampliando a cobertura do escopo.

Coordenação

Distribui áreas do escopo entre agentes para reduzir trabalho duplicado.

Validação e emulação

As capacidades avançadas de validação e emulação dependem da configuração de permissões e limites de efeito do ambiente.

Tipos padrão e personalizados

A equipe da plataforma mantém tipos **padrão**. Organizações também podem criar tipos **personalizados** conforme sua metodologia ou requisitos de conformidade.

Provedores podem ocultar agentes padrão para mostrar apenas os personalizados.

Importar e exportar

Exporte e importe definições JSON para compartilhar configurações entre equipes e organizações.

02.25

Avaliações automáticas

Avaliações automáticas são o modo sem acompanhamento contínuo da avaliação de IA do projeto. A disponibilidade depende da licença, créditos, acesso ao projeto e tipos de agente habilitados.

Antes de começar

Revise escopo incluído e excluído, contexto do ambiente, limites autorizados e créditos. Confira se o tipo de agente é adequado. Clientes usam o contexto dos próprios projetos autorizados; provedores usam a avaliação do cliente correspondente.

Configurar uma avaliação

Na aba **IA** do projeto, o formulário oferece tipo de agente, combinação de modelos quando disponível, modo, profundidade, orçamento de créditos, conector quando necessário e instruções adicionais. Escolha **Automático** para uma execução sem orientação contínua.

As opções atuam dentro das permissões e limites do projeto. Instruções não devem ampliar o escopo autorizado.

Acompanhar o progresso

Consulte etapas, resultados das ferramentas, observações, artefatos e candidatos na transmissão. Uma execução concluída não garante cobertura de todas as vulnerabilidades possíveis nem validade de todos os candidatos.

Controles

O modo automático oferece controles de etapa, repetição e parada. O chat aparece ao assumir a execução no modo assistido, não como controle permanente do modo automático. Parar preserva os resultados registrados; confira status final e transações de crédito.

Revisar os resultados

Revise os candidatos pelas evidências. Aceite achados válidos, rejeite inválidos, solicite provas adicionais ou mescle duplicados quando permitido. Acompanhe a remediação no ciclo normal dos achados.

Consulte [Revisão com IA](#), [Créditos](#) e [Modos](#).

Avaliações recorrentes

Quando disponível, use [Agendamentos de IA](#). Esses agendamentos são separados dos agendamentos internos de monitoramento da superfície.

02.26

Modos de execução

Escolha um modo ao iniciar uma avaliação pela aba **AI Pentest** do projeto. Os controles disponíveis dependem da licença da organização, das suas permissões, das configurações de acesso do cliente e dos perfis e checklists disponíveis no projeto.

Para comparar modos, intenção, local de execução e resultados em detalhes, consulte [Execuções de IA](#). O acesso local é explicado em [Execuções locais](#), e a validação defensiva por plugin em [Execuções purple team](#).

Escolha um modo

Modo	Como funciona	Disponibilidade
Automático	A avaliação segue o perfil selecionado e apresenta o progresso para revisão.	Provedores e clientes cujo projeto permite execuções de IA pelo cliente.
Assistido	Um operador do provedor orienta a avaliação pelo chat e revisa as observações.	Provedores com as permissões necessárias no projeto.
Checklist	A avaliação segue um checklist selecionado e registra a cobertura dos itens.	Exibido quando existe um checklist disponível.

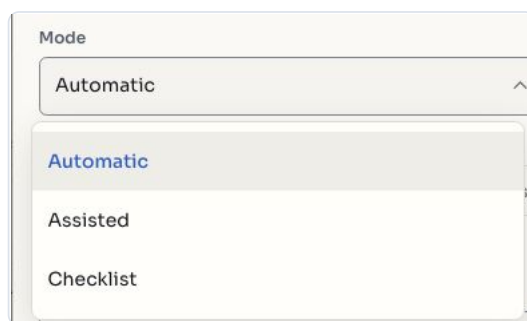


Figura 33 / Opções Automático, Assistido e Checklist

Contas de clientes normalmente iniciam avaliações automáticas e podem não visualizar o seletor de modo. Se um controle não aparecer, peça ao provedor para revisar seu acesso ao projeto e os perfis disponíveis.

Inicie uma avaliação

1. Abra **Projects** e escolha o projeto que você está autorizado a avaliar.
2. Revise o escopo incluído e as exclusões. Sem escopo incluído, a avaliação não executa. Confirme o acesso necessário e o saldo de créditos.
3. Abra **AI Pentest** e clique em **New run**.
4. Selecione um **Profile**. A lista mostra apenas os perfis disponíveis para a categoria do projeto.

- Escolha uma combinação de modelos de IA se esse campo aparecer.
- Escolha **Automatic**, **Assisted** ou **Checklist** quando o seletor estiver disponível. No modo Checklist, selecione também o checklist.
- Nos modos Automático e Checklist, escolha a profundidade: **Lightweight**, **Balanced**, **Deep** ou **Continuous**. Continuous repete o fluxo configurado até atingir seus limites; defina um orçamento de créditos adequado. O modo Assistido não usa o seletor de profundidade.
- Defina o orçamento, escolha um conector se o projeto precisar dele e acrescente instruções sobre o escopo autorizado e os objetivos de revisão.
- Revise a configuração e clique em **Start**. A execução entra na fila e seu progresso aparece no projeto.

New run

Profile

Web application assurance

Model combination

Balanced · 10000 tokens / credit

Mode

Automatic

Assessment intent

Lightweight **Balanced** Deep Continuous

Focus on the issues that most likely exist: the probable vulnerabilities across the in-scope surface, time-boxed.

Budget (credits)

50

Max credits for this run. Default 50. Set 0 for no limit.

Figura 34 / Perfil, modo, intenção da avaliação e orçamento

Internal-network connector

Assessment workspace · Connected

Route this run's internal-network tools through the selected connector. It must be connected when the run reaches the internal stage.

Objective / guidance (optional)

Review the approved inventory and security control baseline. Record observations for human review.

Cancel Start

Figura 35 / Conector, objetivo de revisão e botão Start

Acompanhe e revise

Selecione uma execução para visualizar status, etapa atual, linha do tempo e observações registradas. Execuções automáticas seguem o perfil sem interação contínua pelo chat. No modo Assistido, o operador orienta a avaliação pelo chat. O modo Checklist registra o progresso dos itens selecionados.

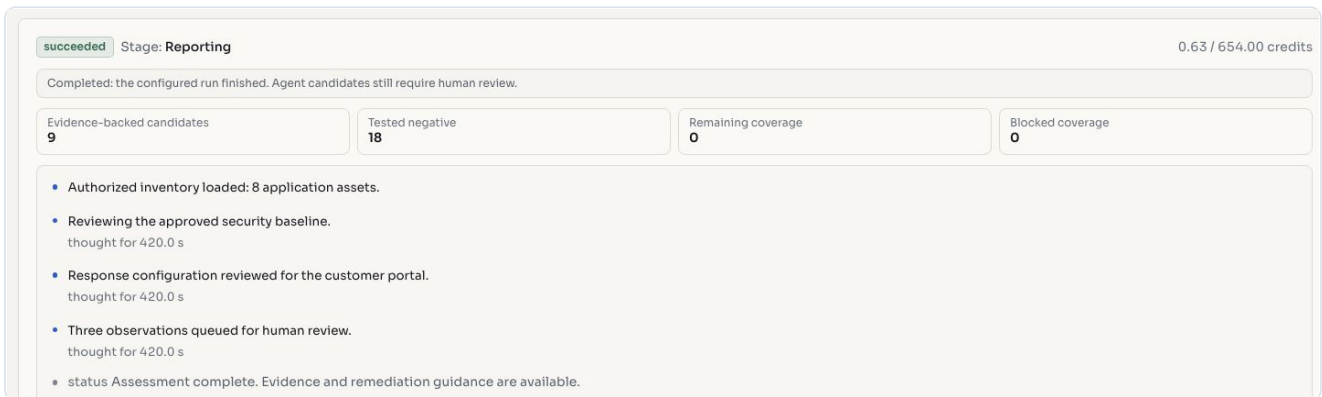


Figura 36 / Progresso e linha do tempo da avaliação

Controles de execução

Os controles exibidos dependem do status, do modo e das suas permissões. Execuções concluídas preservam o histórico para revisão.

Controle	Finalidade
Stop	Interrompe uma execução ativa e preserva achados já registrados.
Skip stage	Solicita a próxima etapa configurada quando disponível.
Take over	Assume uma execução automática ativa no modo Assistido quando permitido.
Redo	Repete uma parte selecionada da avaliação.
Chat	Permite orientar a avaliação no modo Assistido.

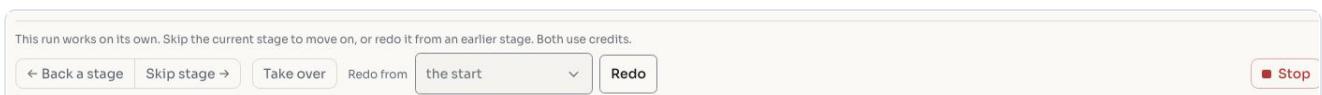


Figura 37 / Controles de uma avaliação ativa

Revise os candidatos antes de aceitá-los. Vincule cada candidato a um achado existente ou crie um novo registro quando necessário. Acompanhe a correção pelo [ciclo de vida dos achados](#). Consulte [avaliações automáticas](#) para os requisitos e o acesso de clientes.

02.27

Checklists

Checklists são guias estruturados para o [modo checklist](#), com os itens que devem ser avaliados.

Edit checklist

Basics

Name

Application security baseline

Description

A reusable review of authentication, authorization, and security configuration.

☒ Enabled

Type **Curated bundles** Coverage template

Walk the bundles and items you author below, one by one.

Client access

Restrict this agent to specific clients. Leave empty to make it available to all.

Search clients to add...

All clients

Bundles 3 items **+ Add bundle**

- 1 Authentication and sessions - 2 items
- 2 Security configuration - 1 item

Cancel **Save changes**

Figura 38 / Editor de checklists

Editor

Defina título, descrição, itens de teste com comportamento esperado e bundles que agrupam verificações por categoria.

Tipos

Checklists regulares

Lista sequencial de itens, classificados como aprovados, reprovados ou não aplicáveis.

Checklists de cobertura

Itens por categoria permitem acompanhar a cobertura mínima necessária antes do relatório.

Padrão e personalizados

Há listas padrão para OWASP Top 10, segurança de APIs e aplicações web. Crie listas próprias para padrões internos, PCI-DSS, SOC 2, HIPAA, aplicações específicas ou requisitos de clientes.

Provedores podem ocultar checklists padrão para ver apenas os personalizados.

Usar checklists

1. Escolha **Checklist** como modo de execução.
2. Selecione a lista na biblioteca.
3. Acompanhe o registro dos resultados de cada item.

Os status documentam a cobertura e apoiam relatórios de conformidade e trilhas de auditoria.

Agendamentos de IA

Agendamentos criam avaliações recorrentes conforme expressões cron.

Edit schedule

Profile

Web application assurance

Mode

Automatic

Assessment intent

Lightweight

Balanced

Deep

Continuous

Focus on the issues that most likely exist: the probable vulnerabilities across the in-scope surface, time-boxed.

Model combination

Select...

Frequency

Every day

Weekly

Twice a month

Monthly

Custom cron

Day of week

Sun

Mon

Tue

Wed

Thu

Fri

Sat

Max credits per run

0

Override the credit budget for each scheduled run. 0 uses the agent type's default.

Objective / guidance (optional)

Cancel

Save

Figura 39 / Editor de agendamento

Criar um agendamento

Campo	Descrição
Tipo de agente	Fluxo de avaliação utilizado
Modo	Automático, assistido ou checklist
Profundidade	Nível de detalhe esperado
Cron	Horário, como 0 2 * * * 1 para segunda-feira às 2h
Projeto	Projeto avaliado

Gerenciar

Ative para criar execuções recorrentes, desative para pausar novas execuções, edite os parâmetros ou exclua o agendamento.

Histórico

Consulte execuções concluídas, falhas ou canceladas, horários de início e fim, quantidade de achados e links para os detalhes.

Casos de uso

- **Validação contínua:** verificações semanais ou mensais após mudanças.
- **Regressão:** retestes periódicos das correções.
- **Conformidade:** evidências de avaliações regulares.

Combine agendamentos e [checklists](#) para avaliações recorrentes padronizadas e resultados auditáveis.

02.29

Conectores

Conectores são agentes de retransmissão que permitem avaliações em redes privadas por uma conexão de saída ao Hashiro.

Como funcionam

O binário `turing-connector` é instalado no ambiente do cliente e estabelece uma conexão **de saída** ao plano de controle.

```
Agente de IA -> Plano de controle Hashiro <- Conector -> Alvos internos
```

Não é necessário abrir portas de entrada para essa conexão.

Modelo de segurança

Recurso	Descrição
Token	Autenticação individual do conector
Fixação de chave TOFU	Confiança no primeiro uso para identificar a chave do servidor
Rotação	Troca de tokens sem reinstalar
Desativação remota	Encerramento da retransmissão
Somente saída	Sem portas de entrada abertas

Capacidades

O conector oferece acesso controlado ao ambiente interno para operações de avaliação e proxy HTTP para aplicações privadas.

Implantação

Use o binário da plataforma com o token da organização em um host com acesso apropriado aos alvos. O conector fica visível no painel do projeto após estabelecer a conexão.

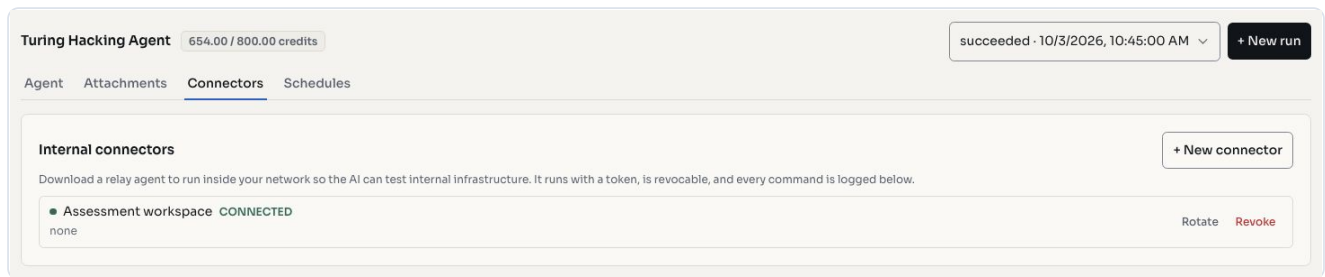


Figura 40 / Painel de atividade do conector

Monitoramento

O painel mostra status online ou offline, último contato e histórico de operações retransmitidas.

Conectores herdam as permissões de rede do host. Escolha um host com acesso adequado ao escopo da avaliação.

Casos de uso

Aplicações internas, ambientes de staging protegidos, APIs e microsserviços privados e avaliações autenticadas de provedores de identidade internos.

02.30

Base de conhecimento

A base reúne referências que os agentes consultam durante avaliações, fornecendo contexto específico do ambiente.

Conteúdo

As entradas são **notas Markdown** sobre arquitetura e tecnologias, autenticação e sessões, regras de negócio, padrões de vulnerabilidade anteriores, configuração do ambiente e metodologia.

Gerenciar entradas

Adicione título e conteúdo, edite informações existentes e exclua material que deixou de ser relevante.

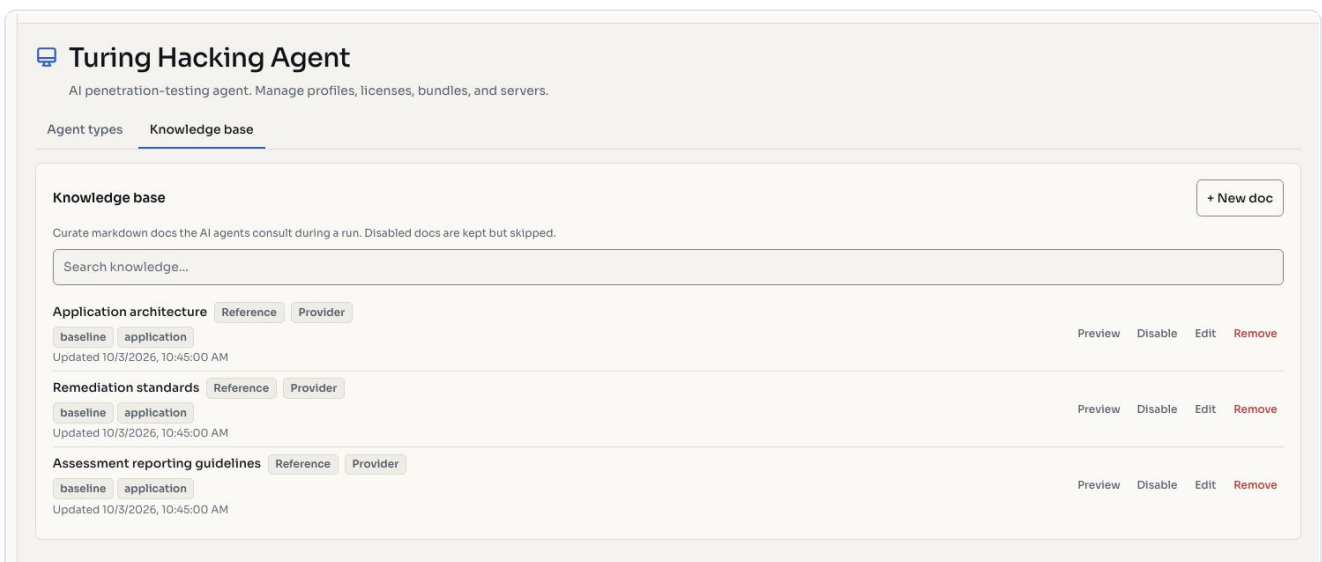


Figura 41 / Painel da base de conhecimento

Uso pelos agentes

Os agentes procuram entradas para entender a arquitetura, aplicar verificações adequadas, evitar caminhos já descartados e focar nas áreas de maior risco. O [modelo estrategista](#) também consulta esse material.

Templates de cobertura

Documentos podem ser vinculados a classes de teste acionadas por palavras-chave. Ao identificar tecnologias, o agente encontra as referências correspondentes.

Atualize a base após as avaliações com lições aprendidas e mudanças da aplicação para manter o contexto atual.

02.31

Créditos e cobrança

Créditos financiam avaliações, revisão assistida por IA e geração de templates, abstraindo os custos de tokens dos LLMs.

Saldos

Saldo	Descrição
Franquia mensal	Concedida conforme a licença e renovada mensalmente
Créditos comprados	Adquiridos pelo Stripe, sem expiração

A franquia mensal é consumida antes dos créditos comprados.

Comprar créditos

1. Abra a seção de avaliações com IA.
2. Acesse **Créditos**.
3. Clique em **Comprar créditos**.
4. Conclua o pagamento no Stripe.

The screenshot shows a panel titled "AI credits" with a balance of 2160.00. It displays "Monthly used" as 0.00 / 1500.00 and "Purchased" as 900.00. A note states: "Monthly credits renew each month and are spent first; purchased credits carry over." At the bottom, there is a "Credits to buy" section with a text input set to "100" and a "Buy credits" button. A footer note says: "Purchased in multiples of 10; charged in your org's currency. Bought credits never expire."

Figura 42 / Painel de créditos

Assinaturas

Assine um plano com franquia mensal, gerencie a assinatura no portal Stripe e consulte seu status, como ativo, pagamento atrasado ou cancelado.

Há uma tolerância de 30 dias para pagamentos atrasados antes do congelamento da cobrança. Mantenha a forma de pagamento atualizada.

Reserva de créditos

Ao iniciar uma execução, créditos são reservados para o custo estimado. A diferença retorna ao saldo se o consumo for menor. Reservas não utilizadas são liberadas no cancelamento.

Acompanhar o uso

O painel mostra saldo mensal e comprado, franquia e data de renovação, transações recentes e consumo por execução.

02.32

Inventário

O Inventário reúne os ativos descobertos em **todos os projetos** da organização em uma interface única com filtros.

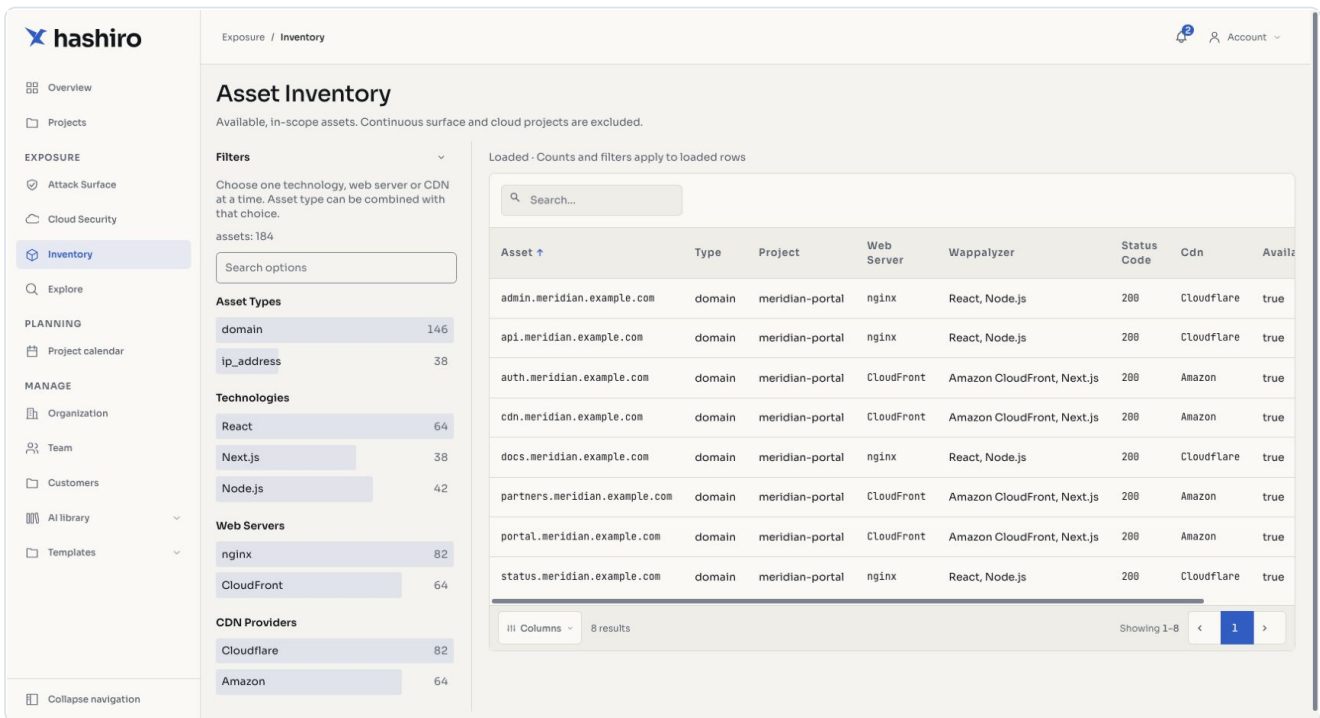


Figura 43 / Inventário com filtros

Filtros por atributos

Filtro	Descrição
Tipo	Domínio, IP, curinga e outros tipos de ativo
Tecnologia	Tecnologias identificadas pelo Wappalyzer, como React, nginx e WordPress
Servidor web	Apache, nginx, IIS e outros servidores
Provedor de CDN	Cloudflare, Akamai e outras redes de entrega de conteúdo

Cada opção mostra uma **barra de contagem** com o número de ativos correspondentes. A pesquisa dentro dos filtros facilita encontrar valores em listas longas.

Tabela de ativos

Coluna	Descrição
Ativo	Hostname, IP ou identificador
Tipo	Classificação do ativo
Projeto	Projeto ao qual pertence
Servidor web	Software identificado
Tecnologias	Tecnologias detectadas pelo Wappalyzer
Código de status	Resposta HTTP da última consulta
CDN	Provedor identificado
Disponibilidade	Indica se o ativo está acessível

Detalhes do ativo

Clique em um ativo para ver a última captura de tela, resposta HTTP completa com cabeçalhos, status e conteúdo, tecnologias, disponibilidade, situação no escopo, serviços e caminhos associados e um link externo para o ativo.

The screenshot displays the Hashiro platform interface for the asset `portal.meridian.example.com`. The interface includes a navigation bar with a "Back to results" link and a status bar showing "Available" and "In Scope". The main content area is divided into several sections:

- Overview:** Contains a "Screenshot" section showing a preview of the website, a "Screenshot" button, and a link to "Open observed host in a new tab".
- Asset Information:** Displays the asset name, IP addresses, and tags.
- HTTP Response:** Shows the status code (200), content length (18.0 KB), page title (Meridian Portal), and web server (CloudFront).
- Technologies Detected:** Lists detected technologies such as Amazon CloudFront and Next.js.
- HTTP Headers:** Shows the content type (text/html; charset=utf-8) and strict transport security (max-age=31536000).

Figura 44 / Detalhes do ativo

02.33

Explorar

A seção Explorar pesquisa ativos, URLs e achados de **todos os projetos** da organização. Localize alvos e padrões sem precisar saber a qual projeto pertencem.

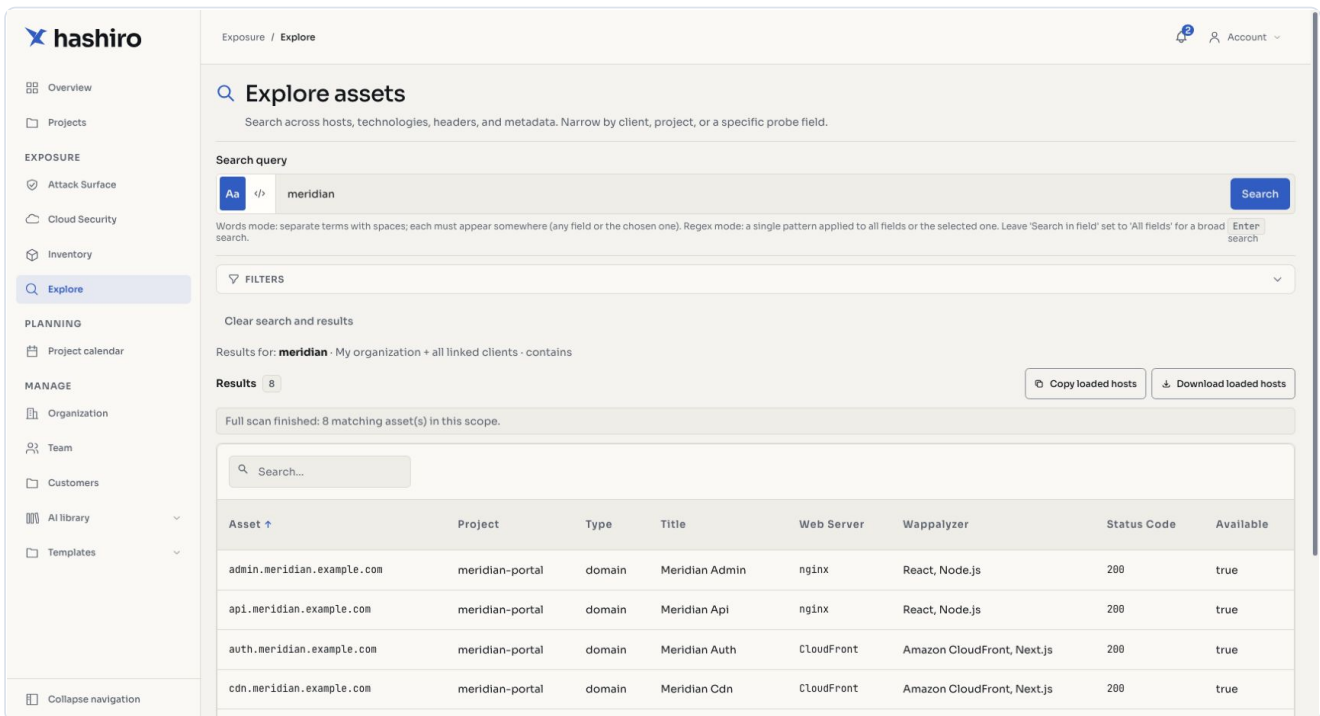


Figura 45 / Interface de pesquisa

Modos de pesquisa

Modo	Descrição
Contém texto	Encontra ativos cujo nome contém o termo informado
Regex	Usa expressões regulares para consultas avançadas

Exemplos

- admin: ativos com “admin” no nome.
- .*\.staging\.example\.com: subdomínios de staging.
- wp-login: páginas de login WordPress entre projetos.
- 10\.0\..*: ativos na faixa 10.0.x.x.

Escopo dos resultados

Organização	Escopo de pesquisa
Provedor	Ativos da própria organização e dos clientes vinculados
Cliente	Somente ativos da própria organização

Resultados

Os resultados mostram metadados, projeto e status da consulta. Abra um resultado para acessar os detalhes do ativo.

02.34

Calendário de projetos

O calendário apresenta uma linha do tempo das avaliações para planejar, agendar e acompanhar os projetos da organização.

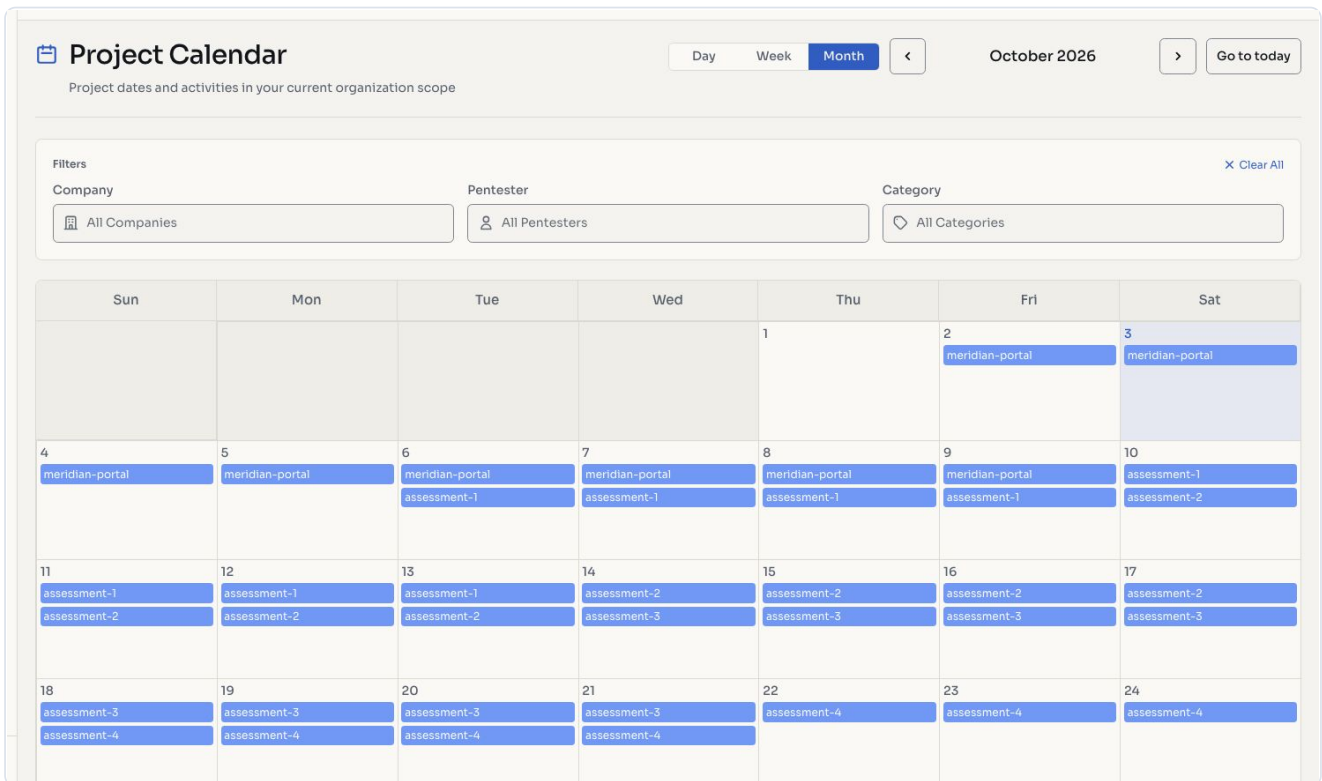


Figura 46 / Calendário mensal de projetos

Visualizações

Visualização	Uso principal
Mês	Distribuição de projetos e planejamento futuro
Semana	Coordenação diária
Dia	Atividades de uma data específica

Navegação

- **Anterior / Próximo:** avance ou recue um período.
- **Hoje:** volte à data atual.

Filtros

Provedores podem filtrar por **empresa** cliente, **pentester** responsável e **categoria** ou tipo de projeto.

Exibição dos projetos

Cada projeto ocupa o intervalo entre as datas de início e fim, mostrando seu nome, duração e sobreposição com outras avaliações.

02.35

Templates

Templates oferecem conteúdo reutilizável para documentar vulnerabilidades, realizar verificações e gerar relatórios PDF, com consistência e menos trabalho repetitivo.

Tipos de template

Templates de vulnerabilidade

Modelos com título, descrição, CVSS, severidade e remediação padronizados para criar achados de qualidade.

Templates Nuclei

Definições YAML para detecção automatizada de vulnerabilidades e verificações específicas da organização em avaliações com IA.

Templates de relatório

Layouts LaTeX que definem cabeçalhos, rodapés, marca, seções e estilos dos relatórios PDF.

Benefícios

- **Consistência:** estrutura e qualidade padronizadas.
- **Eficiência:** campos preenchidos reduzem o tempo de escrita.
- **Padronização:** conhecimento da organização documentado e reutilizável.
- **Marca:** relatórios alinhados à identidade visual.

02.36

Templates de vulnerabilidade

São definições reutilizáveis que preenchem campos comuns de novos achados e organizam o conhecimento da equipe em uma biblioteca pesquisável.

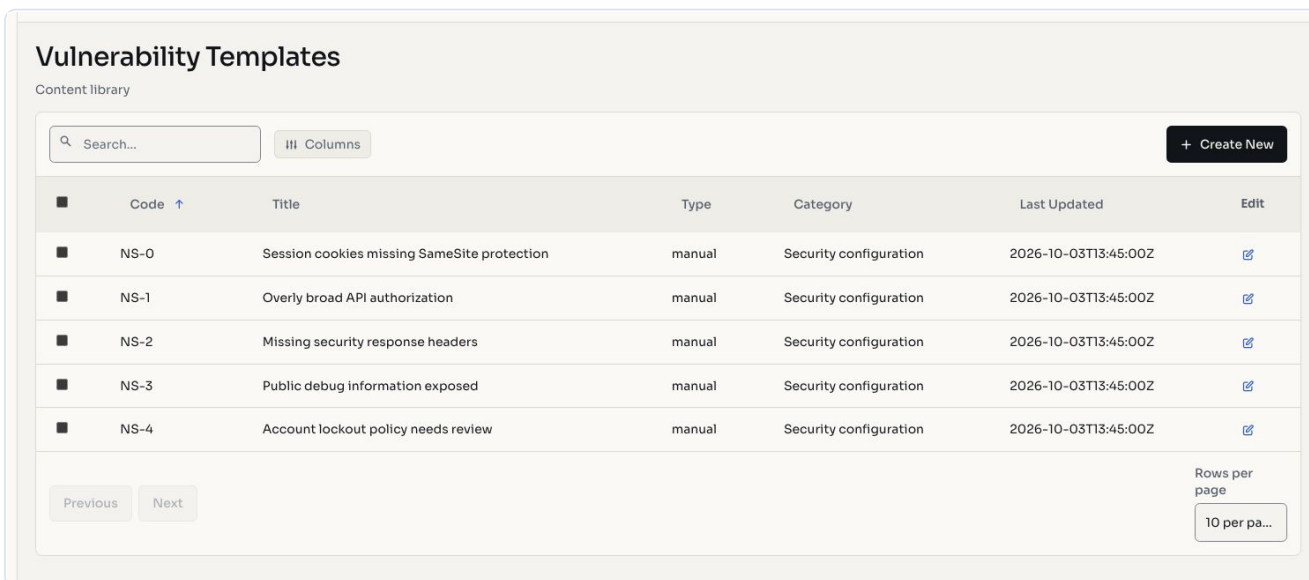


Figura 47 / Biblioteca de templates

Campos de um template

Campo	Descrição
Título	Nome padronizado
Descrição	Explicação detalhada
Severidade	Classificação padrão
CVSS v3.1	Vetor e pontuação previamente calculados
Remediação	Correção ou mitigação
Categoria	Injeção, autenticação, configuração e outras
Referências	Padrões, CVEs e documentação

Biblioteca

Pesquise por palavra ou título, filtre por severidade e categoria, escolha as colunas visíveis e navegue por coleções paginadas.

Criar templates

Criação manual

Preencha os campos para documentar vulnerabilidades específicas da organização.

Geração assistida por IA

Descreva a vulnerabilidade em texto. A IA gera título, descrição, CVSS e remediação.

Use a geração para produzir um rascunho e revise os detalhes conforme os padrões da equipe.

Usar templates

1. Selecione um template ao criar um achado.
2. Os campos recebem o conteúdo do modelo.
3. Adapte os dados ao caso, incluindo evidências do alvo.
4. Salve o achado.

02.37

Templates Nuclei

Templates Nuclei são definições YAML de verificações automatizadas: o que verificar, como avaliar respostas e como classificar resultados.

O que são

Nuclei é uma ferramenta de código aberto que usa templates YAML. O Hashiro a integra às [avaliações com IA](#).

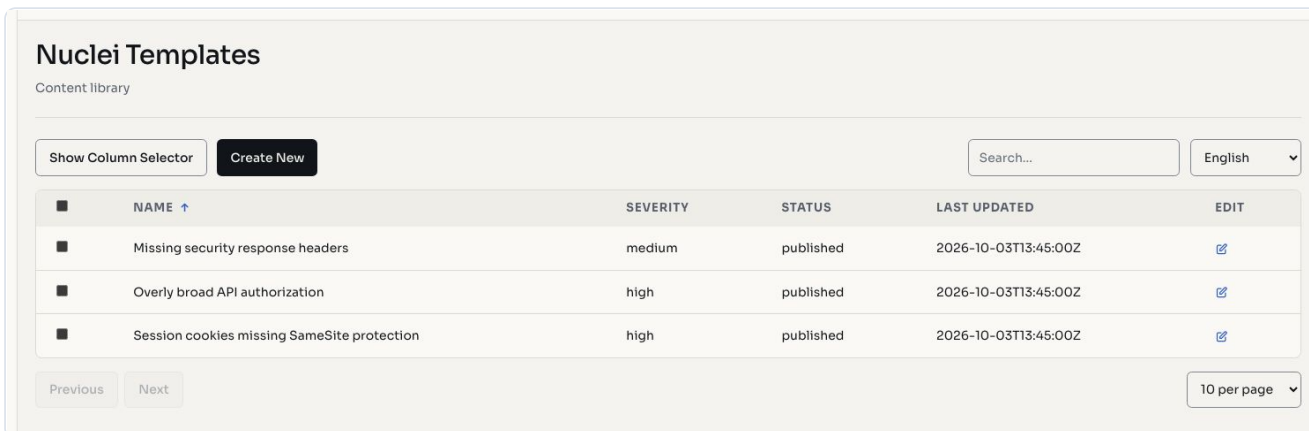
Cada template define requisições, condições de correspondência, extração de evidências, severidade e metadados como CVEs, tags e descrições.

Templates personalizados

Além do catálogo integrado, crie modelos para aplicações próprias, padrões internos de configuração, conformidade e regras de negócio específicas.

Editor YAML

A interface oferece realce de sintaxe e validação.



Nuclei Templates					
Content library					
Show Column Selector		Create New	Search...	English	
	NAME ↑	SEVERITY	STATUS	LAST UPDATED	EDIT
	Missing security response headers	medium	published	2026-10-03T13:45:00Z	✎
	Overly broad API authorization	high	published	2026-10-03T13:45:00Z	✎
	Session cookies missing SameSite protection	high	published	2026-10-03T13:45:00Z	✎

Previous Next 10 per page

Figura 48 / Biblioteca de templates Nuclei

Importação

Importe templates do repositório público Nuclei, de coleções internas ou de outras fontes.

Uso nas avaliações

Agentes de IA selecionam templates relevantes conforme as tecnologias identificadas. Os resultados aparecem como achados com severidade e metadados, seguindo o fluxo regular de revisão e gerenciamento.

02.38

Templates de relatório

Templates LaTeX controlam formato e layout dos relatórios PDF de pentest, incluindo a marca da organização.

Como funciona a geração

1. O Hashiro reúne escopo, achados, CVSS, cadeias, narrativa e remediação.
2. Aplica o template selecionado.
3. Renderiza o documento LaTeX em PDF.
4. Disponibiliza o arquivo para download.

Editor

- **CodeMirror:** realce de sintaxe, números de linha e recolhimento de código.
- **Prévia PDF:** visualização com dados de exemplo durante a edição.
- **Variáveis:** substituição por dados reais do projeto na geração.

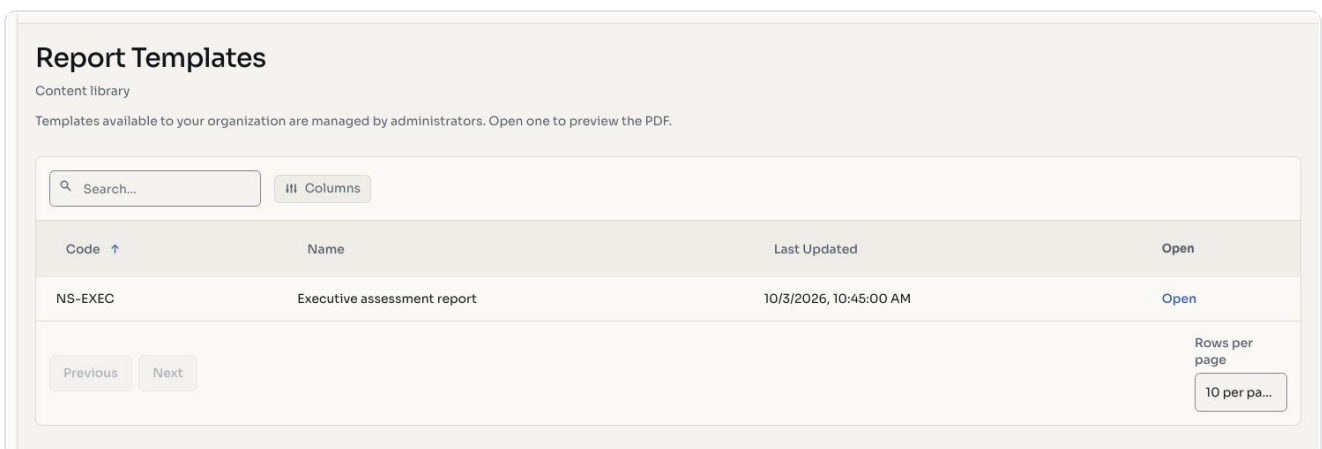


Figura 49 / Biblioteca de templates de relatório

Idiomas

Templates suportam inglês (en) e português (pt). O idioma do projeto determina a variante de títulos, rótulos e textos padrão.

Concessão de acesso

Templates podem ser atribuídos a organizações para relatórios com marcas diferentes, formatos regulatórios específicos ou níveis de serviço.

Gerar relatórios

Selecione um template no projeto. Projetos pequenos podem gerar o arquivo de forma síncrona. Projetos maiores entram em uma fila de processamento e liberam o download ao concluir.

Consulte o status e baixe o relatório quando estiver pronto. Os arquivos são armazenados com segurança e podem ser baixados novamente.

02.39

Links de compartilhamento

Links de compartilhamento permitem acesso **público, sem login**, aos achados de um projeto ou a um achado individual. Use-os para apresentar resultados a pessoas sem conta no Hashiro.

Conteúdo compartilhável

Tipo	Conteúdo
Projeto	Todos os achados, com severidade, status e detalhes
Achado individual	Detalhes completos de uma vulnerabilidade

Criar um link

1. Abra o projeto ou achado.
2. Crie um link com um **rótulo** descritivo, como “Relatório do trimestre”, e uma **data de expiração**.
3. Copie a URL gerada.

Qualquer pessoa com o link pode visualizar o conteúdo sem entrar na plataforma.

Segurança

- **Token:** cada link tem um token único gerado criptograficamente.
- **Armazenamento:** tokens ficam no banco como hashes.
- **Expiração:** o acesso termina na data configurada.
- **Revogação:** desative o link a qualquer momento, com efeito imediato.
- **Somente leitura:** o conteúdo não pode ser alterado.

Os links dão acesso sem autenticação a dados potencialmente sensíveis. Defina expiração e revogue-os quando não forem mais necessários.

Gerenciar links

Liste links ativos, consulte rótulos e datas de expiração e revogue acessos desnecessários na tela de gerenciamento.



PARTE 03

Organização e equipes

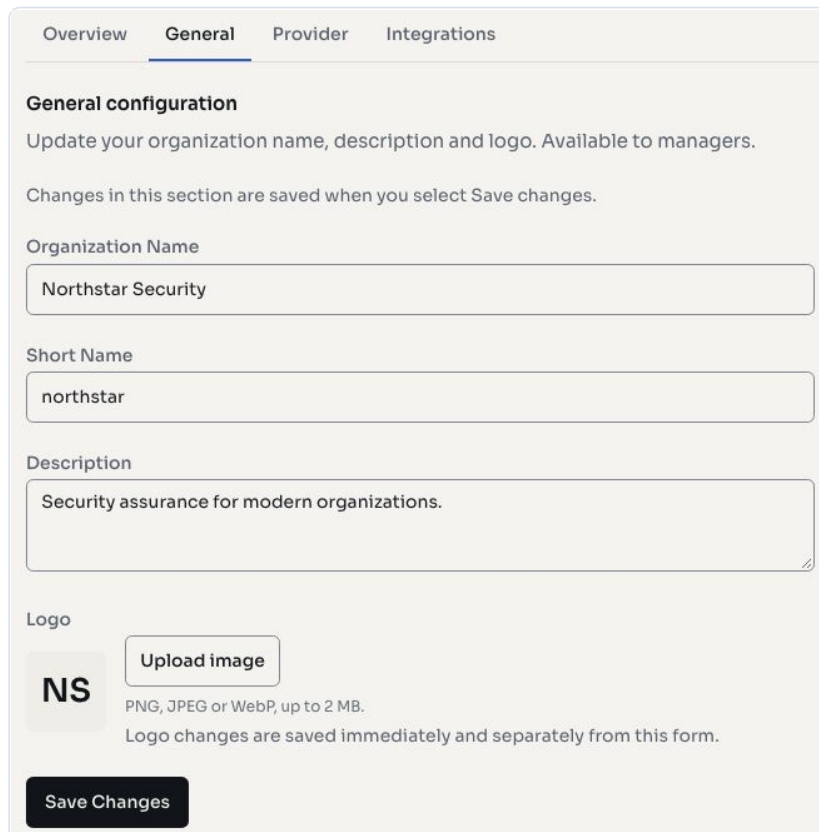
Gerencie pessoas, acesso, clientes e integrações.

CAPÍTULOS / 08

03.01

Gerenciamento da organização

Cada usuário pertence a uma **organização**, unidade de isolamento de dados, cobrança e controle de acesso. Ativos, achados, projetos e configurações são separados entre organizações.



The screenshot shows the 'General' tab of the organization configuration page. It includes fields for 'Organization Name' (Northstar Security), 'Short Name' (northstar), and 'Description' (Security assurance for modern organizations.). There is also a 'Logo' section with an 'Upload image' button and a note about supported formats (PNG, JPEG or WebP, up to 2 MB). A 'Save Changes' button is at the bottom.

Overview **General** Provider Integrations

General configuration
Update your organization name, description and logo. Available to managers.

Changes in this section are saved when you select Save changes.

Organization Name
Northstar Security

Short Name
northstar

Description
Security assurance for modern organizations.

Logo
NS
Upload image
PNG, JPEG or WebP, up to 2 MB.
Logo changes are saved immediately and separately from this form.

Save Changes

Figura 50 / Configurações da organização

Tipos de organização

Provedores

Empresas de segurança, MSSPs e consultorias gerenciam clientes vinculados, acessam os dados autorizados, acompanham indicadores agregados e compartilham templates e tipos de projeto.

Clientes

Clientes têm um ambiente próprio e isolado, vinculado ao provedor para prestação de serviços. Consultam projetos, ativos e achados, gerenciam a equipe dentro dos limites da licença e podem solicitar exclusão da conta.

Organizações independentes

Usam a plataforma sem vínculo com um provedor, conforme os recursos e limites da licença.

Configurações

Abra **Organização** na barra lateral.

Geral

Configure nome, nome curto, descrição, logo usado na interface e nos relatórios e idioma padrão, inglês ou português.

Segurança

Ative a política de OTP para exigir MFA dos membros e restrinja os domínios de email permitidos em convites.

Licenças

Licença	Descrição
Free Business	Recursos básicos com limites reduzidos
Small Business	Gestão de projetos para equipes menores
Medium Business	Maior capacidade conforme os recursos contratados
Custom Business	Limites personalizados
Provider	Gestão de vários clientes
Hunter	Recursos para pesquisadores e bug bounty

A licença determina quantidade de usuários, projetos internos e recursos disponíveis, incluindo avaliações com IA.

Consulte seu administrador ou a equipe comercial para ajustar a licença e os limites.

Criar uma organização

Provedores provisionam clientes pela página **Clientes**. A equipe da plataforma administra a criação e o acesso dos demais tipos de organização.

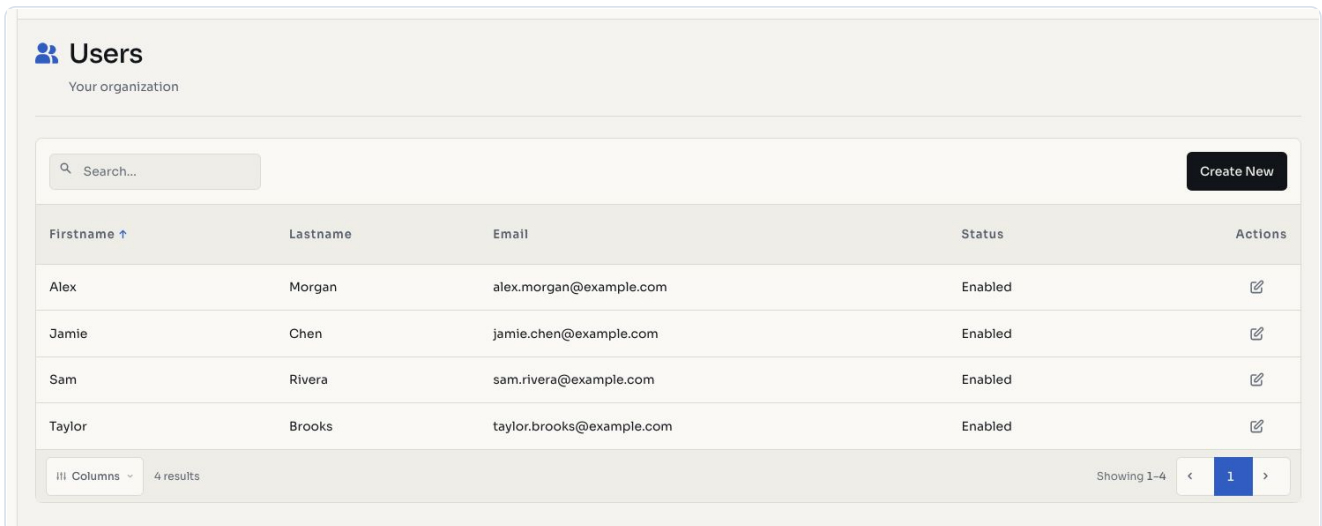
Relacionados

- [Equipe e usuários.](#)
- [Funções e permissões.](#)
- [Clientes.](#)
- [Configurações.](#)

03.02

Equipe e usuários

Convide pessoas, atribua funções e gerencie o acesso à organização.



Firstname ↑	Lastname	Email	Status	Actions
Alex	Morgan	alex.morgan@example.com	Enabled	
Jamie	Chen	jamie.chen@example.com	Enabled	
Sam	Rivera	sam.rivera@example.com	Enabled	
Taylor	Brooks	taylor.brooks@example.com	Enabled	

Figura 51 / Lista de membros

Consultar a equipe

Abra **Equipe** para ver nome, email, função e status de cada membro: ativo, convidado ou provisório.

Convidar usuários

Usuários com permissão de gerenciamento podem:

1. Abrir **Equipe**.
2. Clicar em **Adicionar usuário**.
3. Informar email e nome completo.
4. Escolher uma [função](#).
5. Enviar o convite.

O destinatário recebe um link para definir a senha e ativar a conta.

Restrições de domínio Convites respeitam os domínios de email permitidos pela organização.

Gerenciar convites

Reenvie um convite perdido ou revogue um convite ainda não aceito, conforme as permissões e o estado da organização.

Status dos usuários

Status	Descrição
Ativo	Convite aceito e login disponível
Convidado	Convite enviado, ainda não aceito
Provisório	Conta provisionada, aguardando primeiro acesso

Gerenciar usuários

Editar

Atualize nome, email ou função. As permissões atualizadas são aplicadas nas próximas chamadas à API.

Senha provisória

O gerenciamento de senhas provisórias depende das permissões e do estado da organização. Para recuperar a própria senha, use o fluxo de recuperação no login.

Remover

A remoção revoga o acesso. Ações históricas, comentários e auditoria são preservados.

Minha conta {#my-account}

Abra **Minha conta** no menu do usuário, no canto superior direito.

Figura 52 / Página Minha conta

Perfil

Consulte email e organização e atualize o nome de exibição.

Segurança

Altere sua senha e ative, desative ou redefina a MFA conforme a política da organização.

Chave de API

Gere um token para acesso programático. Consulte [Autenticação](#).

O token é exibido apenas uma vez. Armazene-o com segurança. Gerar outro invalida o anterior.

Aparência

Escolha tema claro ou escuro e idioma inglês ou português.

Notificações

Configure as preferências na aba dedicada. Consulte [Notificações](#).

03.03

Funções e permissões

O Hashiro usa controle de acesso por função. Cada usuário tem uma função na organização. As permissões da função e o escopo da organização são verificados separadamente.

Funções

Administrador da plataforma

A função `administrator` é reservada à organização da equipe Hashiro. Operações globais exigem tanto a licença reservada da plataforma quanto a permissão de administração.

Gerente

A função `manager` gerencia a própria organização, usuários, templates e projetos. É a função de administração usada por provedores e clientes e não concede administração global.

Pentester

A função `pentester` atua nos projetos em que o usuário tem associação explícita. O acesso depende das permissões atribuídas no projeto.

Hunter

A função `hunter` atende pesquisadores de bug bounty, com acesso aos recursos permitidos pela licença e às permissões de templates e projetos.

Visualizador

A função `viewer` permite consultar os projetos em que o usuário é membro, sem acesso de gerenciamento.

Modelo de permissões

Permissões são organizadas por domínio, com criação, listagem, atualização e exclusão. O acesso aos projetos também depende de `AllProjects` ou da associação ao projeto.

Domínio	Exemplos
Projetos	Escopo, membros e detalhes
Ativos	Inventário, URLs e serviços
Achados	Documentação, severidade e status
Templates	Modelos de achados e relatórios
Usuários	Convites, funções e remoção

Domínio	Exemplos
Organização	Configurações, integrações e logo
Avaliações com IA	Execuções e configurações permitidas

Todos os projetos

AllProjects permite acessar os projetos autorizados da organização sem associação individual. Gerentes têm essa permissão; pentesters e visualizadores precisam de associação.

Provedores e clientes

A licença determina o escopo dos dados. **Provedores** podem acessar a própria organização e clientes vinculados, conforme a operação. **Clientes** ficam restritos à própria organização. Ter a mesma função não implica ter o mesmo escopo.

Projetos gerenciados por provedores permanecem somente leitura para clientes nas operações de gestão. Projetos internos gerenciados pelo cliente permitem as ações autorizadas desse cliente.

Escolha de funções Use **Gerente** para administração da organização, **Pentester** para trabalho de avaliação em projetos atribuídos e **Visualizador** para pessoas que precisam consultar resultados. Verifique também as permissões de cada projeto.

03.04

Gerenciamento de clientes

Recurso de provedores Disponível para organizações **provedoras** que prestam serviços a vários clientes.

Use a página **Clientes** para provisionar e acompanhar organizações vinculadas.

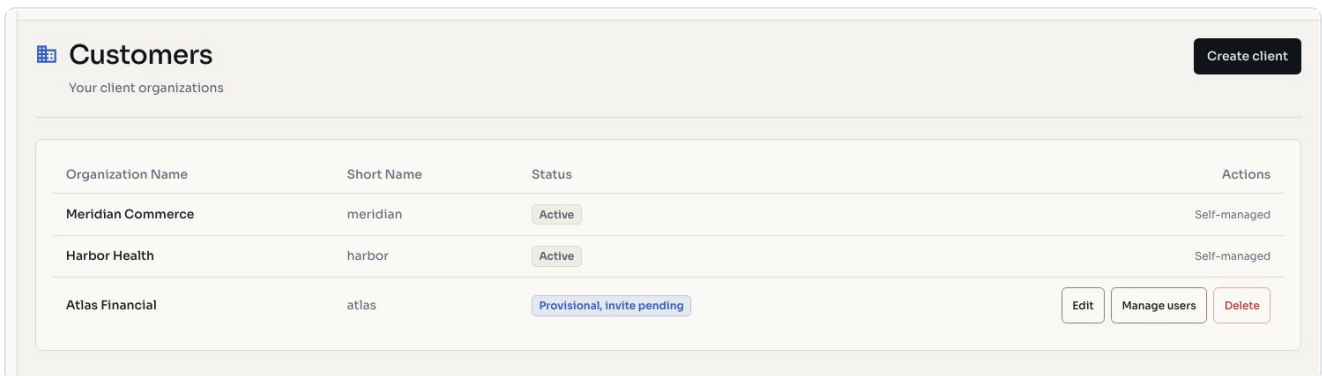


Figura 53 / Lista de clientes

Consultar clientes

Cada registro mostra nome e logo, status (ativo, provisório ou exclusão solicitada), quantidade de usuários e data de criação.

Provisionar um cliente

1. Abra **Clientes** e clique em **Novo cliente**.
2. Informe nome e nome curto da organização, email e nome do contato inicial.
3. Envie o formulário.

A organização é criada e o contato recebe um convite. O usuário inicial gerencia a organização cliente.

Ciclo de vida

Provisionado -> Convite enviado -> Reivindicado -> Ativo
-> Exclusão solicitada -> Excluído

Status	Descrição
Provisionado	Organização criada, convite pendente
Convite enviado	Email enviado ao contato
Reivindicado	Contato aceitou e definiu a senha
Ativo	Organização em operação

Status	Descrição
Exclusão solicitada	Aguardando processamento

Antes de aceitar o convite

Enquanto a organização for provisória, o provedor pode reenviar o convite ou excluir a organização. Após a aceitação, a remoção segue o processo de solicitação de exclusão.

Gerenciar organizações clientes

Usuários

As operações disponíveis dependem do estado da organização e das permissões. Provedores podem consultar os usuários dos clientes vinculados; gerenciamento de convites e senhas provisórias é restrito a clientes ainda não reivindicados.

Configurações

Consulte os detalhes do cliente, como nome, logo, idioma e limites contratados. A disponibilidade de edição depende das permissões e da propriedade da organização.

Acesso

Provedores consultam projetos, ativos e achados de clientes explicitamente vinculados. Esse vínculo não concede acesso a organizações não relacionadas.

O isolamento é aplicado pela plataforma. Um cliente acessa apenas os próprios dados; o vínculo com um provedor não abre acesso a outros clientes.

Solicitações de exclusão

O cliente solicita a exclusão nas configurações da própria organização. A solicitação entra na fila da equipe da plataforma, que aprova ou rejeita. Após aprovação, há um período de retenção antes da remoção permanente, durante o qual a restauração pode ser possível.

03.05

Notificações

O Hashiro oferece **notificações na interface** e **alertas por email**, com controle de categorias e entrega.

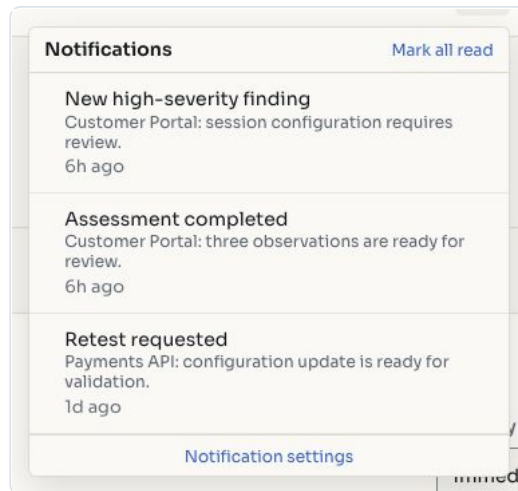


Figura 54 / Painel de notificações

Notificações na interface

O sino na barra superior mostra a contagem não lida. Abra o painel para consultar eventos recentes, navegar ao recurso relacionado, marcar uma ou todas como lidas e excluir registros desnecessários.

Categorias

Segurança

Conclusão ou falha de verificações, novos achados, aumento de severidade e candidatos aguardando revisão.

Conta

Aceitação de convites, novos membros, alterações de função, concessão de créditos e falhas de pagamento.

Sistema

Comunicados da plataforma, manutenção programada e resumos periódicos.

Preferências de email

Use **Configurações de notificações** na conta.

In-app notifications are always on. Choose how you'd like to receive email for each category.

Email delivery
In-app notifications are always on and can't be turned off.

Security
Scans and findings.

Account & organization
Invites, membership, roles, and credits.

System & summaries
Announcements, maintenance, and digests.

Security
Immediate ▾

Account & organization
Immediate ▾

System & summaries
Digest ▾

Digest

Frequency
Daily ▾

Send at
09:00 ▾

Timezone
America/Sao_Paulo ▾

Digest hour uses this timezone: America/Sao_Paulo.

Changes saved.

Figura 55 / Configurações de notificações

Entrega por categoria

Modo	Comportamento
Imediato	Email assim que o evento ocorre
Resumo	Eventos agrupados no horário escolhido
Desativado	Sem email, apenas notificações na interface

Resumos

Escolha frequência diária ou semanal, horário de entrega e fuso horário.

Mantenha eventos críticos como imediatos e agrupe categorias menos urgentes em resumos para reduzir o volume de emails.

Cancelar a inscrição

Cada email inclui um link para desativar a categoria sem precisar entrar na plataforma.

Sugestões

Perfil	Segurança	Conta	Sistema
Pentester ativo	Imediato	Resumo	Desativado
Gestor de equipe	Imediato	Imediato	Resumo
Visualizador	Resumo	Desativado	Desativado

Perfil	Segurança	Conta	Sistema
Conta de automação	Desativado	Desativado	Desativado

03.06

Configurações

A página Configurações reúne atalhos para personalizar o Hashiro e gerenciar a organização.

Aparência

Tema

Alterne entre **claro** e **escuro**. A preferência é salva por dispositivo e aplicada imediatamente.

Idioma

Escolha **inglês** ou **português** para rótulos, mensagens e conteúdo gerado pela interface.

Conta

- **Minha conta:** perfil, senha, token de API e MFA.
- **Notificações:** preferências de email por categoria.

Organização

As opções exigem as permissões de gerenciamento apropriadas:

- **Organização:** nome, logo, descrição, idioma e políticas de segurança.
- **Equipe e usuários:** membros e funções.
- **Integrações:** serviços externos.
- **Licença:** plano e limites.

03.07

Integrações

Integrações conectam o Hashiro às ferramentas da equipe. O gerenciamento é feito na organização por usuários com as permissões adequadas.

Integrações disponíveis

Jira

Sincronização bidirecional entre achados Hashiro e issues Jira, com envio de vulnerabilidades e atualização de status por webhooks.

[Conheça a integração Jira.](#)

Gerenciar integrações

Adicionar

1. Abra **Organização > Integrações**.
2. Clique em **Adicionar integração**.
3. Escolha o tipo.
4. Informe credenciais e configuração.
5. Teste a conexão.
6. Salve.

Testar

Teste novamente após rotações de credenciais ou mudanças no serviço para verificar validade e conectividade.

Editar

Atualize credenciais, URLs ou parâmetros. As alterações entram em vigor imediatamente.

Remover

A exclusão encerra a sincronização. Vínculos existentes são preservados como histórico.

Remover uma integração não exclui dados do serviço externo.

03.08

Integração Jira

A integração sincroniza **bidirecionalmente** achados do Hashiro e issues Jira, conectando equipes de segurança e desenvolvimento.

Edit Integration

Save applies to this integration only.

Name * Jira URL *

Security Remediation https://meridian.example.com/jira

Email * API Token

security@example.com

Leave the token empty to keep the current token. Existing secrets are never shown.

Sync Direction

☒ One-way (Hashiro → Jira) ☐ Two-way (Bidirectional)

Changes in Hashiro are pushed to Jira. Jira changes are not synced back.

Enabled ☒

Cancel Save

Figura 56 / Configuração da integração Jira

Configuração

Pré-requisitos

Uma instância Jira Cloud ou Server, token ou credenciais com acesso aos projetos e permissão de gerenciamento de integrações no Hashiro.

Criar a conexão

1. Abra **Organização > Integrações**.
2. Clique em **Adicionar integração** e escolha **Jira**.
3. Informe URL, como `https://yourteam.atlassian.net`, email da conta e token de API.
4. Clique em **Testar conexão**.
5. Salve.

Token Jira Cloud No Atlassian, abra **Configurações da conta > Segurança > Criar e gerenciar tokens de API**. Gere o token e copie-o para o Hashiro.

Descoberta de projetos

O Hashiro consulta os projetos acessíveis, tipos de issue como Bug, Task e Story, prioridades e campos personalizados.

Mapeamento de campos

Criar um mapeamento

1. Abra os detalhes da integração.
2. Clique em **Adicionar mapeamento**.
3. Escolha projeto Jira e tipo de issue.
4. Relacione título ao resumo Jira, descrição à descrição Jira, severidade à prioridade e outros campos necessários.
5. Salve.

Crie vários mapeamentos para projetos e tipos diferentes.

Editar ou remover

Atualize o mapeamento quando o Jira mudar. A exclusão impede sincronizações futuras e preserva vínculos existentes.

Sincronização

Enviar achados

Use a sincronização completa dos achados mapeados ou envie um achado individual. O Hashiro cria a issue Jira e armazena um vínculo entre os registros.

Comentários de reteste

Envie comentários de reteste ao Jira para informar a equipe de desenvolvimento sobre a verificação.

Webhooks do Jira para Hashiro

1. Abra a aba **Webhooks** da integração.
2. Clique em **Criar webhook**.
3. Copie a URL única gerada.
4. Configure-a nos webhooks do Jira.

Mudanças de status e comentários no Jira atualizam o achado correspondente.

Segurança do webhook A URL contém um identificador único. Não a publique. Regenere ou exclua webhooks quando necessário.

Monitoramento

Status

Consulte total de registros sincronizados, última sincronização e erros.

Histórico

Revise envios, recebimentos, webhooks e falhas para diagnosticar problemas.

Vínculos

Consulte vínculos ativos e remova os que não devem continuar conectados.

Configuração por projeto

Cada projeto Hashiro pode definir qual projeto Jira e qual mapeamento utilizar na sincronização.



PARTE 04

Galileo CLI

Instale, configure e consulte a referência de comandos.

CAPÍTULOS / 05

04.01

Galileo CLI

O Galileo é a interface de linha de comando do Hashiro para projetos, escopo, ativos, URLs, serviços, achados e templates.

Provedores e clientes se conectam a <https://api.hashiro.ai/api/> com um perfil e o próprio token. Os comandos respeitam as mesmas permissões de organização e projeto do console.

Primeiros passos

1. [Instale o Galileo](#) no macOS, Linux ou Windows.
2. [Configure a conexão](#).
3. Liste os projetos autorizados:

```
galileo projects list
galileo projects default my-project
galileo assets list
galileo scan list --json
```

Provedores e clientes

Provedores mantêm os dados das avaliações em projetos e clientes autorizados. Clientes consultam os próprios dados e gerenciam projetos internos nas operações permitidas. O CLI não ignora restrições de acesso ou propriedade.

Recursos

- Criação de projetos, seleção padrão, escopo, narrativa, credenciais e contexto.
- Ativos, caminhos de URL e registros de serviços.
- Documentação de achados e saída JSON.
- Templates de vulnerabilidade reutilizáveis.
- Importação de HackerOne e Intigriti.
- Proxy opcional e atualização automática do binário.

Consulte a [referência de comandos](#) para sintaxe, opções, entradas, saídas e limites, e [importações](#) para as credenciais das plataformas.

04.02

Instalação

O Galileo está disponível para macOS, Linux e Windows. Todos usam <https://api.hashiro.ai/api/> para download.

Consultar a versão

```
curl -fSL https://api.hashiro.ai/api/galileo/latest
```

A resposta JSON contém `version` e o mapa `downloads`. As chaves de arquitetura usam sublinhados. O `download` é um ZIP, não um executável direto. Confira as arquiteturas publicadas na versão atual.

Sistema	Chave de download	Executável no ZIP
macOS Apple Silicon	<code>darwin_arm64</code>	<code>galileo-darwin-arm64</code>
macOS Intel	<code>darwin_amd64</code>	<code>galileo-darwin-amd64</code>
Linux x86-64	<code>linux_amd64</code>	<code>galileo-linux-amd64</code>
Linux ARM64	<code>linux_arm64</code>	<code>galileo-linux-arm64</code>
Windows x86-64	<code>windows_amd64</code>	<code>galileo-windows-amd64.exe</code>

macOS

Execute `uname -m`: `arm64` indica Apple Silicon e `x86_64` indica Intel.

Para Apple Silicon:

```
curl -fSL https://api.hashiro.ai/api/galileo/download/darwin_arm64 -o galileo.zip
unzip -o galileo.zip -d galileo-download
mkdir -p "$HOME/.local/bin"
install -m 755 galileo-download/galileo-darwin-arm64 "$HOME/.local/bin/galileo"
export PATH="$HOME/.local/bin:$PATH"
```

Para Intel, use `darwin_amd64` na URL e instale `galileo-darwin-amd64` do ZIP extraído. Confira os nomes com `unzip -l galileo.zip` se a versão usar outro nome.

Adicione `export PATH="$HOME/.local/bin:$PATH"` ao `~/.zshrc` para manter o PATH em novos terminais.

Linux

Instale `curl` e `unzip`. Execute `uname -m`: use `linux_amd64` para `x86_64` ou `linux_arm64` para `aarch64` / `arm64`.

Para x86-64:

```
curl -fSL https://api.hashiro.ai/api/galileo/download/linux_amd64 -o galileo.zip
unzip -o galileo.zip -d galileo-download
mkdir -p "$HOME/.local/bin"
install -m 755 galileo-download/galileo-linux-amd64 "$HOME/.local/bin/galileo"
export PATH="$HOME/.local/bin:$PATH"
```

Para ARM64, use a chave `linux_arm64` e o executável `galileo-linux-arm64`. Adicione a configuração de `PATH` ao arquivo do shell, como `~/.bashrc` ou `~/.zshrc`.

Windows

Abra o PowerShell. O binário Windows publicado é x86-64. Confira as arquiteturas nos metadados da versão.

```
Invoke-RestMethod https://api.hashiro.ai/api/galileo/latest
Invoke-WebRequest https://api.hashiro.ai/api/galileo/download/windows_amd64 -OutFile galileo.zip
Expand-Archive -Path galileo.zip -DestinationPath galileo-download -Force
$galileoBin = Join-Path $env:LOCALAPPDATA "Hashiro\bin"
New-Item -ItemType Directory -Force $galileoBin
Copy-Item .\galileo-download\galileo-windows-amd64.exe (Join-Path $galileoBin "galileo.exe")
$env:Path = "$galileoBin;$env:Path"
```

Para manter o `PATH`, abra **Editar variáveis de ambiente da sua conta**, edite **Path** do usuário e adicione a pasta `Hashiro\bin` criada em `LocalAppData`. Abra outro terminal após salvar.

Script para macOS e Linux

Você também pode baixar e executar o script de produção:

```
curl -fSL https://api.hashiro.ai/api/install -o install-galileo.sh
bash install-galileo.sh
```

O script detecta a plataforma, baixa e extrai o ZIP e instala o executável. No Windows, use as instruções PowerShell.

Configurar e verificar

Crie o [arquivo de configuração](#) antes de executar o Galileo. Depois:

```
galileo version
galileo projects list
```

Use `galileo version`, não `galileo --version`. Se o comando não for encontrado, confira o `PATH`. Em caso de acesso negado no macOS ou Linux, confira a permissão de execução. Um download 404 indica arquitetura ausente na versão atual; consulte os metadados.

Atualizar

```
galileo update
```

A atualização automática fica ativa por padrão. Desative com `no_update = true` ou `--no-update`; o comando explícito `update` continua funcionando. O script também pode reinstalar a versão mais recente.

04.03

Configuração

Provedores e clientes usam a mesma API de produção, <https://api.hashiro.ai/api/>. Configure um perfil para sua organização. O token determina identidade, organização, licença e permissões; o nome do perfil não concede acesso de provedor.

Criar o arquivo

Gere um token em **Minha conta** no [console Hashiro](#). Crie o arquivo:

Sistema	Arquivo
macOS / Linux	~/.config/galileo/config.toml
Windows	%USERPROFILE%\config\galileo\config.toml

No macOS ou Linux:

```
mkdir -p ~/.config/galileo
$EDITOR ~/.config/galileo/config.toml
chmod 600 ~/.config/galileo/config.toml
```

No PowerShell do Windows:

```
New-Item -ItemType Directory -Force "$env:USERPROFILE\config\galileo"
notepad "$env:USERPROFILE\config\galileo\config.toml"
```

Cole a configuração e substitua o valor de exemplo pelo token:

```
current_project = ""
no_update = false
no_skills_update = true

[[profiles]]
name = "hashiro"
default = true
api_address = "https://api.hashiro.ai/api/"
api_key = "REPLACE_WITH_YOUR_API_TOKEN"
```

Referência dos campos

Campo	Significado
current_project	Identificador do projeto padrão. Vazio até selecionar um projeto.
no_update	true desativa atualização automática do binário. O padrão é false.
no_skills_update	true desativa atualização automática dos arquivos de comandos Claude Code instalados.

Campo	Significado
[[profiles]]	Entrada de array TOML, obrigatória mesmo com um perfil.
name	Nome local da conexão.
default	true seleciona o perfil padrão.
api_address	Use sempre <code>https://api.hashiro.ai/api/</code> . O Galileo normaliza o sufixo da API.
api_key	Token gerado pelo usuário.
proxy	URL opcional de proxy HTTP. Omita quando não precisar.
default_project	Identificador opcional dentro do perfil, carregado como projeto atual.

Não use `[profiles.default]`, `url`, `token` ou `current_program`, pois não correspondem ao formato atual.

Acesso de provedores e clientes

Tokens de provedor acessam os dados próprios e de clientes vinculados nas operações permitidas. Tokens de cliente ficam restritos à própria organização. O endereço da API é igual para ambos. Associação e propriedade do projeto também determinam as operações disponíveis.

Verificar a conexão

```
galileo config profile list
galileo config profile default
galileo projects list
```

O perfil padrão aparece com *. A listagem é somente leitura e mostra projetos autorizados.

Selecionar projeto padrão

```
galileo projects default my-project
galileo projects default
galileo assets list
galileo assets list --project another-project
galileo projects default --unset
```

`--project` escolhe o projeto de uma chamada. Mantenha `current_project` no nível principal para usar o comando de seleção; `default_project` no perfil pode definir novamente o projeto a cada carregamento.

Proxy

```
galileo config proxy set http://127.0.0.1:8080
galileo config proxy unset
```

Os comandos alteram o perfil padrão. O proxy não muda a instância nem as permissões.

Gerenciar a configuração

`galileo config set ./config.toml` copia um arquivo TOML para o caminho padrão. Não define pares de chave e valor. Crie o arquivo padrão antes da primeira chamada, pois a configuração é carregada antes de executar comandos.

Com um perfil, não é necessário alternar conexões. Se adicionar outra identidade na mesma instância, `galileo config profile default NAME` define o padrão e `--profile NAME` seleciona um perfil para uma chamada.

Atualizações e diagnóstico

Use `galileo --no-update projects list` para pular a atualização automática em uma chamada. `galileo update` verifica explicitamente mesmo com atualizações automáticas desativadas.

Problema	Verificação
Arquivo ausente	Crie no caminho indicado para o sistema.
Erro de TOML	Use <code>[[profiles]]</code> , strings entre aspas e opções globais antes do perfil.
Falha de autenticação	Troque o exemplo por um token válido; gerar outro invalida o anterior.
Acesso negado	Confira função, licença, associação ao projeto e vínculo da organização.
Projeto incorreto	Use <code>--project</code> ou revise o padrão salvo.

O arquivo contém uma credencial. Mantenha-o privado e fora do controle de versão.

04.04

Referência de comandos

Esta referência cobre comandos da API de projetos para provedores e clientes. Token e permissões do projeto determinam o acesso. Comece pela [configuração](#).

Ajuda e opções globais

```
galileo --help
galileo assets service --help
galileo --no-update --no-skills-update projects list
```

Opção	Significado
--help, -h	Mostra ajuda.
--profile NAME	Seleciona o perfil de uma chamada. Um perfil basta na configuração padrão.
--no-update	Pula atualização automática do binário.
--no-skills-update	Pula atualização dos arquivos Claude Code instalados.

Use o identificador de `projects list`. Comandos por projeto aceitam `--project / -p` ou o padrão salvo.

Exceção: em `projects create`, `-p` escolhe a plataforma.

Versão e atualização

```
galileo version
galileo update
```

`version` mostra a versão instalada e pode informar uma mais recente. `update` atualiza somente o binário, mesmo com atualização automática desativada.

Configuração

```
galileo config set ./config.toml
galileo config profile list
galileo config profile default
galileo config profile default hashiro
galileo config profile default --unset
galileo config proxy set http://127.0.0.1:8080
galileo config proxy unset
```

`config set` copia um arquivo TOML, sem pares de chave e valor. Crie o arquivo padrão primeiro. `profile default` consulta o perfil sem argumento e troca com um nome. `--unset` remove a marca de padrão e passa a usar o primeiro perfil.

Exemplos de projetos

```
galileo projects create my-project --platform pentest --tag owner=security
galileo projects list --all
galileo projects default my-project
galileo projects inscope --project my-project --type domain example.com
galileo projects outscope --project my-project --type domain excluded.example.com
galileo projects inscope --project my-project
galileo projects inscope --project my-project --rm example.com
```

Aliases de projetos: project, program, programs, p. list aceita ls / l; create aceita c / add; remove aceita rm / r. Coloque curingas entre aspas para impedir expansão pelo shell.

Narrativa, credenciais, contexto e cadeias

```
galileo projects narrative --project my-project
galileo projects narrative --project my-project < narrative.md
galileo projects context --project my-project < context.md
galileo projects credentials --project my-project < credentials.md
galileo projects chains --project my-project
```

Sem conteúdo, consulta o campo Markdown. Argumentos ou entrada padrão substituem o campo. chains é somente leitura. Clientes não recebem acesso de edição em projetos do provedor por usar esses comandos.

Exemplos de ativos, URLs e serviços

```
galileo assets insert --project my-project app.example.com
galileo assets list --project my-project --unavailable --show-status-code
galileo assets view --project my-project app.example.com
galileo assets path --project my-project --add https://app.example.com/health
galileo assets path --project my-project https://app.example.com
galileo assets service --project my-project --asset app.example.com
galileo assets service --project my-project --json
galileo assets service --project my-project --add --asset app.example.com --port 443 --protocol tcp --state open
```

Aliases de ativos: asset, domain, domains. path aceita paths / dir; service aceita services. Inserção, consulta individual e remoção recebem o nome do ativo como argumento. Não existem assets insert --asset nem assets path --path.

Exemplos de achados

```
galileo scan add --project my-project --asset app.example.com --title "Missing security header"
--severity low --description "Observed during review" --remediation "Configure the required header"
galileo scan list --project my-project --info
galileo scan list --project my-project --id FINDING_ID
galileo scan list --project my-project --json
```

Aliases: scans, issue, issues. Consulte com scan list --id; não existe scan view. scan add --raw aceita um objeto JSON na entrada padrão. --requests-file aceita pares JSON, como [{"texto da requisição", "texto da resposta"}].

Templates e importação

```
galileo templates list --verbose
galileo templates view TEMPLATE_CODE_OR_ID
galileo import hackerone
galileo import intigriti
```

Aliases de templates: template, t. view aceita show. Configure as credenciais das plataformas conforme [Importações](#).

Notificações

```
galileo notify FINDING_ID --discord
```

Configure [discord] com channel e token. Informe IDs nos argumentos ou linhas na entrada padrão. --id não é consumido pela implementação. O envio Slack não está implementado, embora a opção apareça na ajuda.

Arquivos opcionais para Claude Code

```
galileo gen-skills ./claude-config
```

Grava uma seção delimitada em CLAUDE.md e comandos em commands/. O diretório padrão é ~/ .claude. Altera arquivos locais; --no-skills-update impede atualizações automáticas posteriores.

Tabelas de comandos e opções

Opções de array podem ser repetidas, como --tag owner=security --tag env=test. Opções inteiras recebem números e booleanas podem ser definidas explicitamente como false.

galileo projects create NAME

Cria um projeto. NAME é posicional; -p significa plataforma neste comando.

Opção	Descrição
--platform VALUE / -p	Plataforma do projeto, como pentest, hackerone ou intigriti.
--inactive / -i	Cria ou lista projetos inativos.
--type VALUE	Tipo do registro.
--tag VALUE / -t	Tag no formato chave=valor; pode ser repetida.
--raw	Lê um objeto JSON da entrada padrão.

galileo projects list

Lista projetos autorizados.

Opção	Descrição
--all / -a	Inclui ou remove todos os registros, conforme o comando.
--inactive / -i	Cria ou lista projetos inativos.
--tag VALUE / -t	Tag no formato chave=valor; pode ser repetida.
--value VALUE / -v	Valor da tag usada como filtro.

galileo projects remove NAME

Exclui um projeto após confirmação.

Opção	Descrição
--yes / -y	Dispensa confirmação da exclusão.

galileo projects default [NAME]

Consulta ou define o projeto padrão.

Opção	Descrição
--unset	Limpa a seleção padrão.

galileo projects inscope [TARGET...]

Consulta, adiciona ou remove entradas dentro do escopo.

Opção	Descrição
--project VALUE / -p	Identificador do projeto; substitui o projeto padrão.
--rm / -r	Remove a entrada indicada.
--bounty VALUE / -b	Elegibilidade para recompensa, como string true ou false.
--type VALUE	Tipo do registro.
--wildcard / -w	Filtra entradas curinga.
--domains / -d	Filtra domínios.
--tier VALUE	Nível numérico do ativo.

Opção	Descrição
--issues VALUE / -i	Quantidade conhecida de achados.
--tag VALUE / -t	Tag no formato chave=valor; pode ser repetida.

galileo projects outscope [TARGET...]

Consulta, adiciona ou remove exclusões.

Opção	Descrição
--project VALUE / -p	Identificador do projeto; substitui o projeto padrão.
--bounty VALUE / -b	Elegibilidade para recompensa, como string true ou false.
--rm / -r	Remove a entrada indicada.
--type VALUE	Tipo do registro.
--wildcard / -w	Filtra entradas curinga.
--domains / -d	Filtra domínios.
--tier VALUE	Nível numérico do ativo.
--issues VALUE / -i	Quantidade conhecida de achados.
--tag VALUE / -t	Tag no formato chave=valor; pode ser repetida.

galileo assets insert HOST...

Insere hostnames por argumentos ou entrada padrão.

Opção	Descrição
--project VALUE / -p	Identificador do projeto; substitui o projeto padrão.
--httpx	Solicita consulta HTTPX para obter metadados.
--screenshot / -s	Solicita captura de tela com HTTPX.
--tag VALUE / -t	Tag no formato chave=valor; pode ser repetida.
--ipaddress VALUE / -i	Endereço IP associado; pode ser repetido.
--available / -a	Marca disponibilidade; o padrão na inserção é false.

Opção	Descrição
--scheme VALUE	Protocolo do endereço, como https.
--port VALUE	Número da porta.
--title VALUE	Título do registro ou da página.
--status-code VALUE	Código de resposta HTTP; -1 indica não informado.
--content-length VALUE	Tamanho do conteúdo; -1 indica não informado.
--favicon VALUE	Hash do favicon.
--lines VALUE	Contagem de linhas; -1 indica não informado.
--words VALUE	Contagem de palavras; -1 indica não informado.
--location VALUE	Cabeçalho HTTP Location.
--webserver VALUE	Servidor web identificado.
--body VALUE	Hash do corpo da resposta.
--jarm VALUE	Impressão digital JARM.
--b64screenshot VALUE	Captura de tela codificada em Base64.
--cdn VALUE	CDN identificada.
--header VALUE	Cabeçalho no formato chave=valor; pode ser repetido.
--wappalyzer VALUE	Tecnologia identificada; pode ser repetida.

galileo assets list

Lista ativos disponíveis; inclua indisponíveis com --unavailable.

Opção	Descrição
--project VALUE / -p	Identificador do projeto; substitui o projeto padrão.
--domains / -d	Filtra domínios.
--unavailable / -u	Inclui ativos indisponíveis.
--show-wappalyzer	Exibe as tecnologias na listagem.
--show-status-code	Exibe o código HTTP na listagem.

Opção	Descrição
<code>--show-title</code>	Exibe o título na listagem.

galileo assets view HOST

Mostra um ativo e sua captura de tela disponível.

Opção	Descrição
<code>--project VALUE / -p</code>	Identificador do projeto; substitui o projeto padrão.

galileo assets remove HOST...

Remove ativos selecionados; `--all` remove todos no projeto escolhido.

Opção	Descrição
<code>--project VALUE / -p</code>	Identificador do projeto; substitui o projeto padrão.
<code>--all</code>	Inclui ou remove todos os registros, conforme o comando.
<code>--yes / -y</code>	Dispensa confirmação da exclusão.

galileo assets path [URL...]

Lista caminhos por padrão; use `--add`, `--rm` ou `--rm-all` para alterar. Informe URLs completas.

Opção	Descrição
<code>--project VALUE / -p</code>	Identificador do projeto; substitui o projeto padrão.
<code>--add</code>	Adiciona um registro.
<code>--rm</code>	Remove a entrada indicada.
<code>--rm-all</code>	Remove todos os caminhos do ativo.
<code>--httpx</code>	Solicita consulta HTTPX para obter metadados.
<code>--source VALUE / -s</code>	Origem dos dados.
<code>--tag VALUE / -t</code>	Tag no formato chave=valor; pode ser repetida.
<code>--title VALUE</code>	Título do registro ou da página.

Opção	Descrição
--status-code VALUE	Código de resposta HTTP; -1 indica não informado.
--content-length VALUE	Tamanho do conteúdo; -1 indica não informado.
--favicon VALUE	Hash do favicon.
--lines VALUE	Contagem de linhas; -1 indica não informado.
--words VALUE	Contagem de palavras; -1 indica não informado.
--location VALUE	Cabeçalho HTTP Location.
--webserver VALUE	Servidor web identificado.
--body VALUE	Hash do corpo da resposta.
--jarm VALUE	Impressão digital JARM.
--b64screenshot VALUE	Captura de tela codificada em Base64.
--cdn VALUE	CDN identificada.
--header VALUE	Cabeçalho no formato chave=valor; pode ser repetido.
--wappalyzer VALUE	Tecnologia identificada; pode ser repetida.

galileo assets service [HOST]

Lista serviços registrados; --add adiciona um registro. Este comando não verifica portas.

Opção	Descrição
--project VALUE / -p	Identificador do projeto; substitui o projeto padrão.
--asset VALUE / -a	Ativo relacionado; em notas pode ser repetido.
--add	Adiciona um registro.
--list / -l	Lista os serviços registrados.
--port VALUE	Número da porta.
--protocol VALUE	Protocolo de rede, como tcp ou udp.
--banner VALUE	Descrição ou banner do serviço.
--state VALUE	Estado da porta: open, closed ou filtered.

Opção	Descrição
--script VALUE / -s	Resultado de script associado; pode ser repetido.
--tag VALUE / -t	Tag no formato chave=valor; pode ser repetida.
--hosts	Lista hosts disponíveis.
--services	Exibe hostname:porta e serviço.
--service VALUE	Filtra pelo nome do serviço.
--ports	Exibe lista consolidada de portas.
--port-filter VALUE	Filtra portas separadas por vírgulas.
--json	Produz saída JSON.
--csv	Produz saída CSV.

galileo scan add

Cria um achado por opções ou objeto JSON na entrada padrão com --raw.

Opção	Descrição
--project VALUE / -p	Identificador do projeto; substitui o projeto padrão.
--notify	Notifica o achado após criação.
--severity VALUE	Severidade do achado ou filtro.
--asset VALUE	Ativo relacionado; em notas pode ser repetido.
--title VALUE	Título do registro ou da página.
--description VALUE	Descrição do achado.
--notified	Marca como já notificado.
--fp	Marca como falso positivo.
--source VALUE	Origem dos dados.
--cve VALUE	Identificador CVE.
--reference VALUE	URL de referência; pode ser repetida.
--tag VALUE	Tag no formato chave=valor; pode ser repetida.

Opção	Descrição
--template VALUE	Identificador do template.
--demonstration VALUE	Documentação de validação do achado.
--observation VALUE	Observação ou contexto.
--type VALUE	Tipo do registro.
--category VALUE	Categoria do registro ou filtro.
--remediation VALUE	Orientações de remediação.
--retest-demonstration VALUE	Documentação do reteste.
--requests-file VALUE	Arquivo JSON com pares de requisição e resposta.
--raw	Lê um objeto JSON da entrada padrão.

galileo scan list

Lista achados; --id seleciona um registro e --json produz saída estruturada.

Opção	Descrição
--project VALUE / -p	Identificador do projeto; substitui o projeto padrão.
--title VALUE	Título do registro ou da página.
--id VALUE	Identificador para consulta; em notify não substitui os argumentos.
--asset VALUE	Ativo relacionado; em notas pode ser repetido.
--severity VALUE	Severidade do achado ou filtro.
--info	Inclui achados informativos.
--json	Produz saída JSON.

galileo scan remove ID...

Exclui achados pelos IDs nos argumentos ou entrada padrão.

Opção	Descrição
--project VALUE / -p	Identificador do projeto; substitui o projeto padrão.

Opção	Descrição
--yes / -y	Dispensa confirmação da exclusão.

galileo templates list

Lista templates de vulnerabilidade disponíveis à conta.

Opção	Descrição
--verbose / -v	Exibe detalhes dos templates.

galileo templates view CODE_OR_ID

Consulta um template por código ou ID.

galileo notify ID...

Notifica achados por ID via Discord. Slack não está implementado.

Opção	Descrição
--slack	Opção presente, mas envio Slack não implementado.
--discord	Ativa envio Discord; padrão true.
--id VALUE	Identificador para consulta; em notify não substitui os argumentos.

Entradas, saídas e falhas

Comandos de texto aceitam linhas na entrada padrão quando indicado. --raw espera um objeto JSON, não uma lista. Use `scan list --json` e `assets service --json` para saída estruturada. Não presuma que toda saída é JSON nem que todo erro de validação produz um código de saída diferente de zero; confira as mensagens. Exclusões pedem confirmação, salvo com --yes. Confira projeto e IDs antes de usar opções em lote.

04.05

Importações

O Galileo importa programas de bug bounty autorizados para projetos Hashiro e converte alvos incluídos e excluídos em entradas de escopo. Usa o perfil Hashiro normal e credenciais separadas da plataforma de origem.

Pré-requisitos

Configure a [conexão Hashiro](#) e use uma conta com permissão para criar projetos. Adicione as seções necessárias ao `config.toml`:

```
[hackerone]
username = "YOUR_HACKERONE_USERNAME"
api_key = "YOUR_HACKERONE_API_TOKEN"

[intigrity]
api_key = "YOUR_INTIGRITI_API_TOKEN"
```

Essas credenciais são diferentes de `api_key` do Hashiro. Inclua apenas as plataformas utilizadas.

HackerOne

```
galileo import hackerone
```

Alias: `h1`. O Galileo usa usuário e token HackerOne, consulta programas disponíveis, cria projetos e importa alvos dentro e fora do escopo. Confira erros por programa na saída.

Intigrity

```
galileo import intigrity
```

Alias: `int`. O Galileo usa o token bearer Intigrity, consulta programas acessíveis e importa informações e escopo. Programas sem escopo utilizável ou identificador podem ser ignorados.

Verificar o resultado

```
galileo projects list
galileo projects inscope --project PROGRAM_NAME
galileo projects outscope --project PROGRAM_NAME
```

Compare as entradas com as regras atuais do programa. A importação não substitui autorização nem restrições da origem. Pode haver conclusão parcial; confira erros antes de repetir.

Mapeamento do escopo

Domínios e curingas viram entradas correspondentes. Aplicativos móveis e código-fonte mantêm sua classificação quando compatível. Revise tipos incomuns após importar, sem presumir equivalência completa entre plataformas.



PARTE 05

Referência da API

Conecte aplicações usando a base da API pública.

CAPÍTULOS / 06

05.01

API Hashiro

A API básica atende **provedores e clientes** na mesma instância de produção:

```
https://api.hashiro.ai/api/
```

Os caminhos desta referência são relativos à base. `/users/me` corresponde a `https://api.hashiro.ai/api/users/me`.

Autenticação

Envie seu token no cabeçalho `X-HASHIRO-TOKEN`:

```
curl --fail-with-body \  
-H "X-HASHIRO-TOKEN: $HASHIRO_TOKEN" \  
https://api.hashiro.ai/api/users/me
```

Defina `HASHIRO_TOKEN` no ambiente com o token gerado em **Minha conta** no [console](#). Consulte [Autenticação](#).

Escopo de provedores e clientes

Conta	Dados autorizados
Provedor	Organização própria e clientes explicitamente vinculados, quando a rota permite
Cliente	Organização própria, incluindo resultados publicados das avaliações do provedor

Função, licença, associação e propriedade do projeto são verificados separadamente. Informar o ID de um cliente não concede acesso irrestrito. Clientes não podem editar a configuração dos projetos do provedor nas rotas básicas de escrita. Projetos gerenciados pelo cliente permitem as operações autorizadas dos próprios responsáveis.

Referência

- [Projetos e escopo](#).
- [Ativos, URLs e serviços](#).
- [Achados e revisão](#).
- [Organizações e usuários](#).

Requisições e respostas

Envie Content-Type: application/json para JSON. Endpoints de arquivos usam o formato específico, que pode ser multipart ou dados de imagem em JSON.

Listas podem ser arrays, detalhes são objetos e escritas retornam mensagens ou identificadores. Não existe um envelope data universal.

Erros normalmente contêm error ou message. Confira o status HTTP antes de tratar a resposta como sucesso.

Status	Significado
400	Parâmetros ou corpo inválidos
401	Autenticação ausente ou inválida
403	Permissão, licença ou acesso à organização insuficientes
404	Recurso inexistente ou invisível à conta
409	Conflito, inclusive versão de revisão desatualizada
429	Limite de requisições atingido
5xx	Falha no servidor ou serviço externo

Paginação

Listas básicas usam page e pageSize, não limit. A primeira página é 1. Métricas de projetos usam 10 itens por padrão; ativos e achados usam 100. O servidor pode limitar páginas grandes. Nem toda lista tem contagem total ou metadados compartilhados.

```
curl --fail-with-body -H "X-HASHIRO-TOKEN: $HASHIRO_TOKEN" \  
'https://api.hashiro.ai/api/scans/?project=my-project&page=1&pageSize=100'
```

Consulte páginas seguintes até não haver mais registros. Caminhos por projeto usam o identificador, não o nome de exibição.

Limites e novas tentativas

Login, OTP, recuperação de senha e ações assistidas por IA têm limites próprios. Em 429, respeite o cabeçalho de nova tentativa quando houver ou aguarde progressivamente. Não repita escritas automaticamente, pois podem duplicar dados ou cobrar novamente ações de IA.

05.02

Autenticação

Use **tokens de API** em integrações e no Galileo. O console web usa cookies de sessão HTTP-only.

Token de API

1. Entre no [Hashiro](#).
2. Abra **Minha conta**.
3. Gere a chave de API e copie-a imediatamente.
4. Armazene como variável privada ou segredo.

O token é exibido uma vez. Gerar outro invalida o anterior. As permissões e o escopo são herdados do usuário.

```
curl --fail-with-body \  
-H "X-HASHIRO-TOKEN: $HASHIRO_TOKEN" \  
https://api.hashiro.ai/api/organizations/me
```

Provedores e clientes usam o mesmo cabeçalho e a mesma base de produção. O Galileo lê `api_key` na [configuração](#).

POST `/users/generateToken` gera um token substituto para o usuário autenticado. Como rotaciona uma credencial, use a interface para a configuração inicial e não chame esse endpoint apenas para testar conectividade.

Sessões do navegador

POST `/auth/signin` aceita:

```
{  
  "email": "user@example.com",  
  "password": "your-password"  
}
```

A resposta pode exigir MFA ou alteração de senha antes do acesso completo. `access_token` e `refresh_token` gerenciam a sessão. O refresh token renova o acesso expirado. GET `/auth/logout` encerra a sessão.

MFA

Método	Caminho	Finalidade
GET	<code>/auth/otp/create</code>	Iniciar configuração TOTP na sessão autenticada
POST	<code>/auth/otp/create</code>	Validar configuração e ativar MFA
POST	<code>/auth/otp/validate</code>	Concluir MFA no login

Método	Caminho	Finalidade
POST	/users/otp/enable	Iniciar configuração autenticada
POST	/users/otp/reset	Redefinir a própria MFA quando permitido
POST	/users/otp/disable	Desativar quando a política permitir

Use o console para o fluxo completo. A verificação OTP tem limite de tentativas e pode ser obrigatória pela política da organização.

Recuperar e alterar senha

Método	Caminho	Corpo
POST	/auth/password-reset/request	<code>{"email": "user@example.com"}</code>
POST	/auth/password-reset/confirm	<code>{"token": "RESET_TOKEN", "password": "NEW_PASSWORD"}</code>
POST	/users/me/change-password	<code>{"currentPassword": "CURRENT_PASSWORD", "newPassword": "NEW_PASSWORD"}</code>

A recuperação usa o token enviado por email. Usuários provisionados podem precisar trocar a senha no primeiro acesso.

Aceitar convite

POST /auth/register recebe o token de convite e os campos necessários. Ativa uma conta convidada e não é um endpoint geral para criação pública de organizações.

Falhas comuns

Um token inválido falha na autenticação. Um token válido ainda pode receber 403 por falta de autorização. Regenere tokens expostos e atualize as integrações correspondentes.

05.03

Projetos e escopo

Todos os caminhos são relativos a <https://api.hashiro.ai/api/> e exigem X-HASHIRO-TOKEN.

Acesso

Leituras exigem acesso geral aos projetos ou associação ao projeto. Criação exige permissão geral. Escritas exigem as permissões correspondentes e propriedade do provedor ou um projeto gerenciado pelo próprio cliente. O cliente não altera a configuração de projetos do provedor.

Rotas

Método	Caminho	Operação
GET	/projects/metrics	Listar projetos autorizados com métricas
GET	/projects/:projectName	Consultar projeto
PUT	/projects/:projectName	Criar projeto
PATCH	/projects/:projectName	Atualizar detalhes
DELETE	/projects/:projectName	Solicitar exclusão do projeto e dados associados
GET	/projects/:projectName/:scope	Consultar inscope ou outscope
POST	/projects/:projectName/:scope	Adicionar entradas de escopo
PATCH	/projects/:projectName/:scope/asset/:assetId	Atualizar entrada
DELETE	/projects/:projectName/:scope/asset/:assetId	Excluir entrada
PATCH	/projects/:projectName/members	Atualizar membros
PATCH	/projects/:projectName/displayName	Atualizar nome de exibição
POST	/projects/:projectName/report	Solicitar PDF
GET	/projects/:projectName/report/status	Consultar status do PDF
GET	/projects/:projectName/report/download	Baixar PDF pronto
GET	/projects/:projectName/download/:fileFormat	Baixar relatório no formato compatível

Listar projetos

Use GET `/projects/metrics?page=1&pageSize=10`, a rota de listagem usada pelo Galileo. GET `/projects/` não é o endpoint documentado de listagem.

Criar

Use um identificador com letras minúsculas, números e hífen, com até 50 caracteres. Não confunda identificador e nome de exibição. Corpo de exemplo para PUT `/projects/my-project`:

```
{
  "platform": "pentest",
  "type": "private",
  "status": "active",
  "definitions": {"category": "internal"}
}
```

Provedores associam clientes autorizados por `customer_id`. Clientes não podem selecionar outra organização. Categorias e limites dependem das configurações e da licença.

Escopo

`:scope` é `inscope` ou `outscope`. Corpo para POST `/projects/my-project/inscope`:

```
{
  "assets": [
    {"asset": "app.example.com", "asset_type": "domain"}
  ]
}
```

Os tipos incluem `wildcard`, `domain`, `ip_address`, `cdir`, `ios`, `android`, `source` e `other`. `cdir` é a grafia existente na API para CIDR. Use o ID retornado para atualizar ou excluir uma entrada.

Relatórios

As rotas atendem projetos de avaliação compatíveis gerenciados pelo provedor. Projetos do cliente não recebem automaticamente acesso a relatórios do provedor. Solicite, consulte o status e baixe após a conclusão. Downloads retornam arquivos, não JSON. Templates dependem da organização.

Exclusão

A exclusão inicia a remoção dos dados associados. Considere-a irreversível e aguarde a conclusão antes de reutilizar o identificador.

05.04

Ativos, URLs e serviços

Use `https://api.hashiro.ai/api/` com `X-HASHIRO-TOKEN`. IDs e projetos precisam pertencer ao escopo autorizado.

Rotas

Método	Caminho	Operação
GET	<code>/assets/</code>	Listar ativos com project, asset, filter, page e pageSize
GET	<code>/assets/:assetId</code>	Consultar ativo pelo ID
POST	<code>/assets/:projectName</code>	Criar ativos de um array JSON
PUT	<code>/assets/:projectName</code>	Rota alternativa de criação
POST	<code>/assets/search</code>	Pesquisar inventário autorizado
GET	<code>/assets/inventory/stats</code>	Consultar estatísticas dos filtros
GET	<code>/assets/paths</code>	Listar caminhos por project e asset opcional
GET	<code>/assets/:assetId/paths</code>	Listar caminhos de um ativo
GET	<code>/assets/paths/:pathId</code>	Consultar caminho
POST	<code>/assets/:projectName/paths</code>	Adicionar caminhos com asset na query
POST	<code>/assets/:projectName/services</code>	Adicionar serviços com asset na query
POST	<code>/assets/:projectName/restart-probe</code>	Solicitar nova consulta
DELETE	<code>/assets/</code>	Excluir ativos conforme os filtros exigidos
DELETE	<code>/assets/project/:projectName</code>	Excluir todos os ativos do projeto
DELETE	<code>/assets/paths</code>	Excluir caminhos selecionados
DELETE	<code>/assets/path/:pathId</code>	Excluir caminho pelo ID

Consultar ativos

```
curl --fail-with-body -H "X-HASHIRO-TOKEN: $HASHIRO_TOKEN" \  
  'https://api.hashiro.ai/api/assets/?project=my-project&filter=all&page=1&pageSize=100'
```

`filter` seleciona disponibilidade; `all` inclui indisponíveis. Rotas de detalhes usam o ID, enquanto a query `asset` usa o nome. Registros incluem `id`, `asset`, `project`, `type`, `available`, `scope`, `probe`, `ip_address` e `services`.

Criar ativos

Envie um array a `POST /assets/my-project`:

```
[
  {"asset": "app.example.com", "type": "domain", "available": true}
]
```

Criação exige associação, licença e propriedade compatíveis. Exclusão e nova consulta têm restrições adicionais de provedor e projeto. Permissão de leitura não implica escrita.

Caminhos de URL

`POST /assets/my-project/paths?asset=app.example.com` aceita um array de registros com `path`, `url`, `source`, `probe` e `tags`. No Galileo, informe URLs completas; a API separa caminho e URL.

Serviços

`POST /assets/my-project/services?asset=app.example.com` aceita um array:

```
[
  {"port": 443, "protocol": "tcp", "state": "open", "service": "https"}
]
```

A operação registra observações conhecidas e não inicia uma verificação de portas. Consulte os serviços nos detalhes do ativo. Estados incluem `open`, `filtered`, `closed` e `unknown`.

Pesquisa de inventário

`POST /assets/search` pesquisa o inventário autorizado. Provedores podem consultar clientes vinculados; clientes consultam somente a própria organização. A query não permite escolher uma organização não relacionada.

05.05

Achados e revisão

Os endpoints usam /scans, o nome existente do recurso. Use X-HASHIRO-TOKEN com `https://api.hashiro.ai/api/`.

Acesso

Leitura depende da associação ou acesso geral aos projetos. Criação, alteração e exclusão exigem permissão de pentester ou gestão e projeto permitido do provedor ou do próprio cliente. Clientes revisam candidatos públicos elegíveis, sem acesso a rascunhos privados do provedor ou achados de outras organizações.

Rotas

Método	Caminho	Operação
GET	/scans/	Listar achados com project, page e pageSize
GET	/scans/:scanId	Consultar achado
PUT	/scans/:projectName	Criar achado
POST	/scans/:projectName	Atualizar achado com ID no corpo
DELETE	/scans/:projectName/:scanId	Excluir achado
POST	/scans/:projectName/bulk-status	Alterar status em lote
POST	/scans/:projectName/bulk-delete	Excluir em lote
POST	/scans/:projectName/:scanId/review	Revisar candidato com versão esperada
POST	/scans/:projectName/:scanId/ai/demonstration	Gerar rascunho de documentação
POST	/scans/:projectName/:scanId/ai/demonstration/apply	Aplicar rascunho revisado
POST	/scans/:projectName/:scanId/ai/merge	Propor mesclagem para revisão

Criar um achado

Envie a PUT /scans/my-project:

```
{
  "title": "Missing security header",
  "asset": ["app.example.com"],
  "severity": "low",
```

```
"description": "Observed during the assessment",  
"remediation": "Configure the required header"  
}
```

asset é um array, mesmo para um host. Campos opcionais incluem observação, demonstração, remediação, referências, requisições, CVSS e tags. Referências precisam ser URLs HTTP ou HTTPS. cwe e owasp também são URLs quando informados.

A criação retorna success e Ids; preserve os identificadores. Novos achados de clientes recebem status conforme a política do servidor, que pode não aceitar rascunhos para essa conta.

Atualizar

POST /scans/my-project exige id, title e asset não vazio. Consulte o registro, preserve esses campos e envie as alterações permitidas. Decisões de status de candidatos pendentes usam a rota de revisão.

Status em lote

```
{  
  "ids": ["FINDING_ID"],  
  "status": "pending_retest"  
}
```

Envie a POST /scans/my-project/bulk-status. O limite é 500 IDs. bulk-delete recebe ids sem status e remove permanentemente os registros autorizados.

Revisar candidatos

Use a versão retornada pelo candidato e envie a decisão com expected_review_version. Um conflito exige consultar o registro atualizado. Revisão e mesclagem dependem da função, projeto e visibilidade. Geração assistida pode consumir créditos; revise antes de aplicar.

Consulte [Ciclo de vida](#) e [Revisão com IA](#) para o fluxo na interface.

05.06

Organizações e usuários

Provedores e clientes usam `https://api.hashiro.ai/api/` com `X-HASHIRO-TOKEN`. Permissões de organização não dão acesso a organizações arbitrárias.

Rotas

Método	Caminho	Operação
GET	<code>/users/me</code>	Consultar próprio usuário
PATCH	<code>/users/me</code>	Atualizar perfil
PATCH	<code>/users/me/appearance</code>	Atualizar tema e idioma
GET	<code>/organizations/me</code>	Consultar própria organização
PATCH	<code>/organizations/me</code>	Atualizar própria organização
GET	<code>/organizations/customers</code>	Listar vínculos autorizados
GET	<code>/organizations/:organizationId</code>	Consultar organização autorizada
POST	<code>/organizations/clients</code>	Provedor: criar cliente e usuário inicial
DELETE	<code>/organizations/:organizationId</code>	Provedor: excluir cliente provisionado ainda não reivindicado
POST	<code>/organizations/me/deletion-request</code>	Solicitar exclusão da própria organização
GET	<code>/users/</code>	Listar usuários da organização
GET	<code>/users/:organizationId</code>	Listar usuários de organização vinculada permitida
PUT	<code>/users/</code>	Criar usuário autorizado
POST	<code>/users/:organizationId/:userId</code>	Atualizar usuário autorizado
POST	<code>/users/:organizationId/:userId/delete</code>	Remover usuário autorizado
POST	<code>/users/:organizationId/:userId/resent-invite</code>	Reenviar convite de cliente provisório
POST	<code>/users/:organizationId/:userId/revoke-invite</code>	Revogar convite provisório
POST	<code>/users/:organizationId/:userId/reset-password</code>	Redefinir senha provisória permitida

Método	Caminho	Operação
POST	/organizations/me/logo	Enviar logo
DELETE	/organizations/me/logo	Remover logo
GET	/organizations/me/integrations/	Listar integrações
POST	/organizations/me/integrations/	Criar integração
GET	/organizations/me/integrations/:integrationId	Consultar integração
PATCH	/organizations/me/integrations/:integrationId	Atualizar integração
DELETE	/organizations/me/integrations/:integrationId	Remover integração
POST	/organizations/me/integrations/:integrationId/test	Testar integração

Consulte sua identidade

Use /users/me e /organizations/me para identificar usuário, organização e permissões. O gerenciamento de um cliente vale para a própria organização. Vínculos de provedor só permitem operações autorizadas para os clientes relacionados.

Provisionar um cliente

Um provedor com permissão de criação envia a POST /organizations/clients:

```
{
  "name": "Example Client",
  "shortname": "example-client",
  "initial_user": {
    "email": "manager@example.com",
    "firstname": "Example",
    "lastname": "Manager",
    "mode": "invite"
  }
}
```

O modo de convite envia um link para definir a senha. A organização fica provisória até ser reivindicada. Convites e exclusão pelo provedor dependem desse estado. Após aceitação, a exclusão segue solicitação do cliente e revisão da plataforma.

Usuários

Criação e gestão exigem a permissão User correspondente e acesso à organização. Redefinição, revogação e reenvio pelo provedor atendem contas provisórias elegíveis, sem controle permanente sobre credenciais de clientes já reivindicados.

A função regular de gerenciamento é `manager`. `administrator global` é reservado à equipe Hashiro, não a provedores ou clientes.

Integrações

As rotas são da própria organização e exigem permissões e licença compatíveis. Credenciais são dados de entrada; não espere receber segredos em consultas posteriores. Consulte [Jira](#) para mapeamento e sincronização.