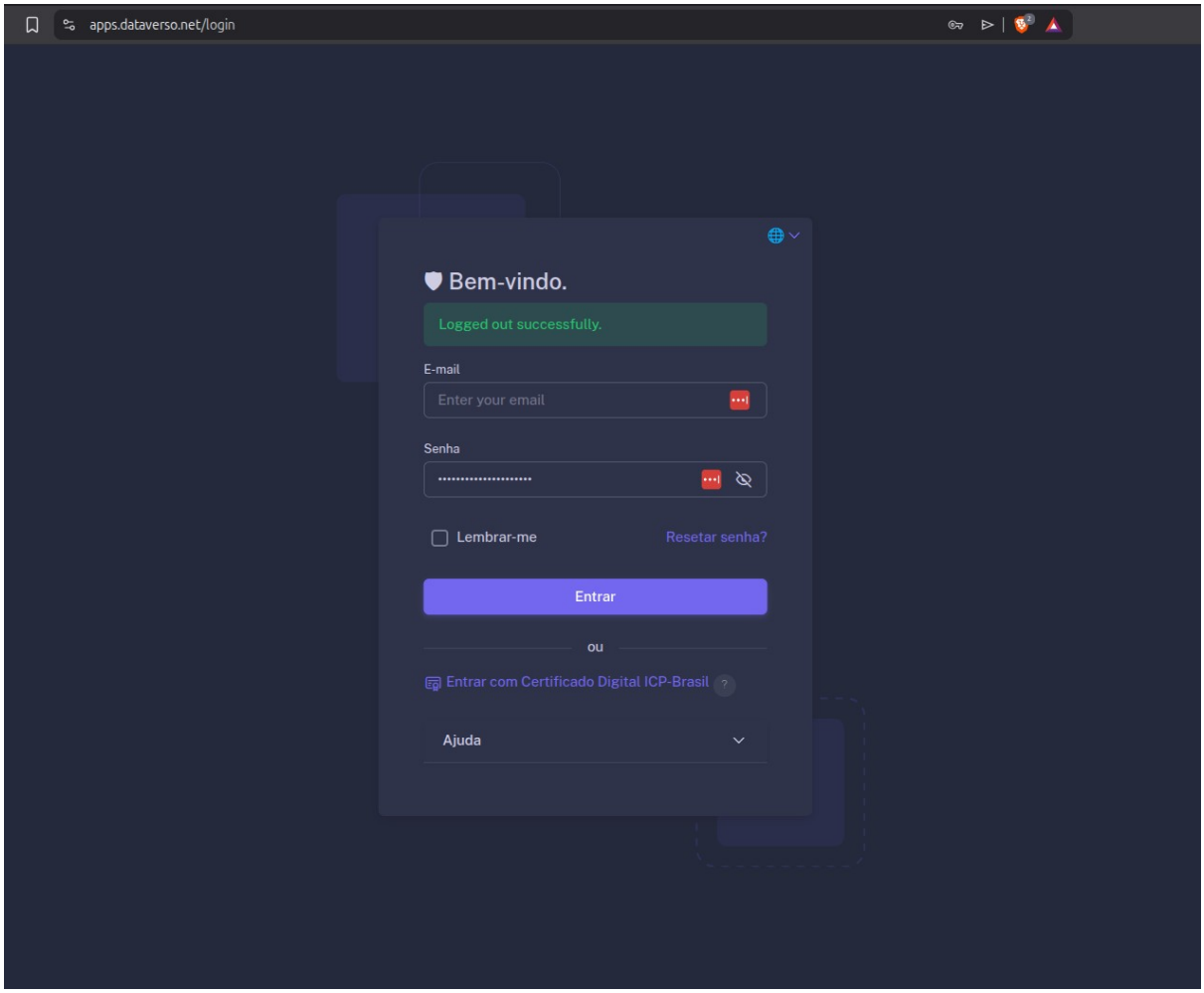
2. REQUISITOS GERAIS

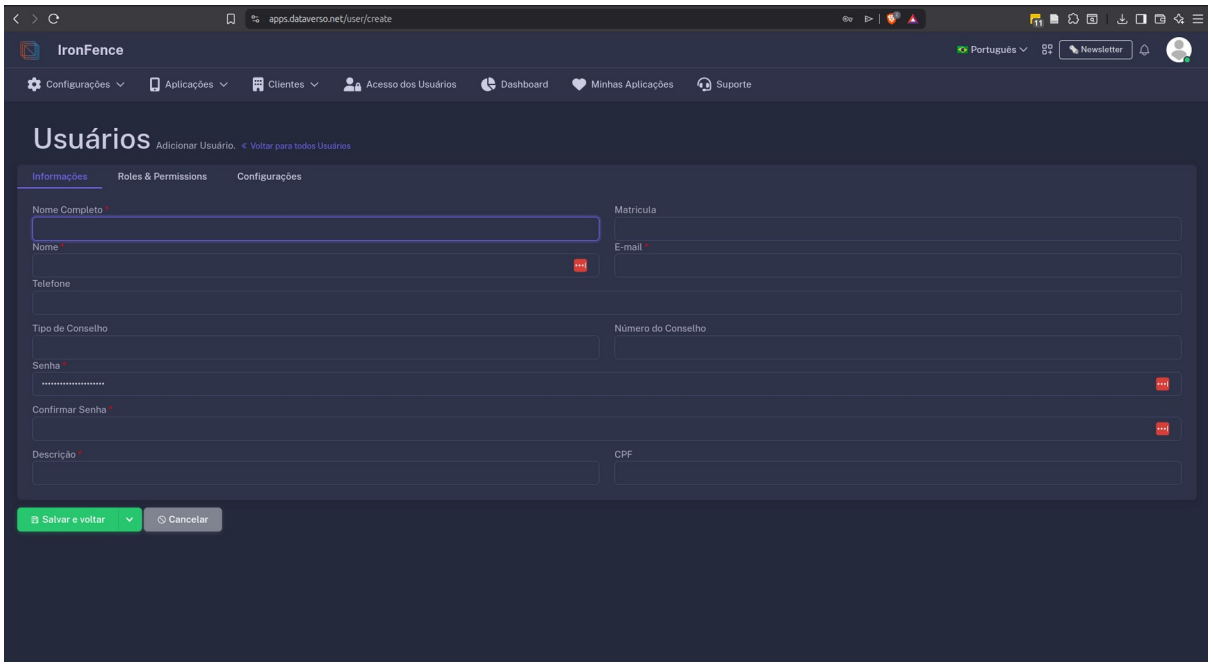
2.1. Os serviços deverão ser prestados fora das dependências do Banco do Nordeste.



https://apps.dataverso.net/login

2.2. O serviço de CTI deverá prover uma console de acesso para que o Banco e as equipes do seu SOC (serviços de SOC e SIEM não fazem parte do escopo desta contratação) possam consultar

as informações de inteligência de ameaças cibernéticas.



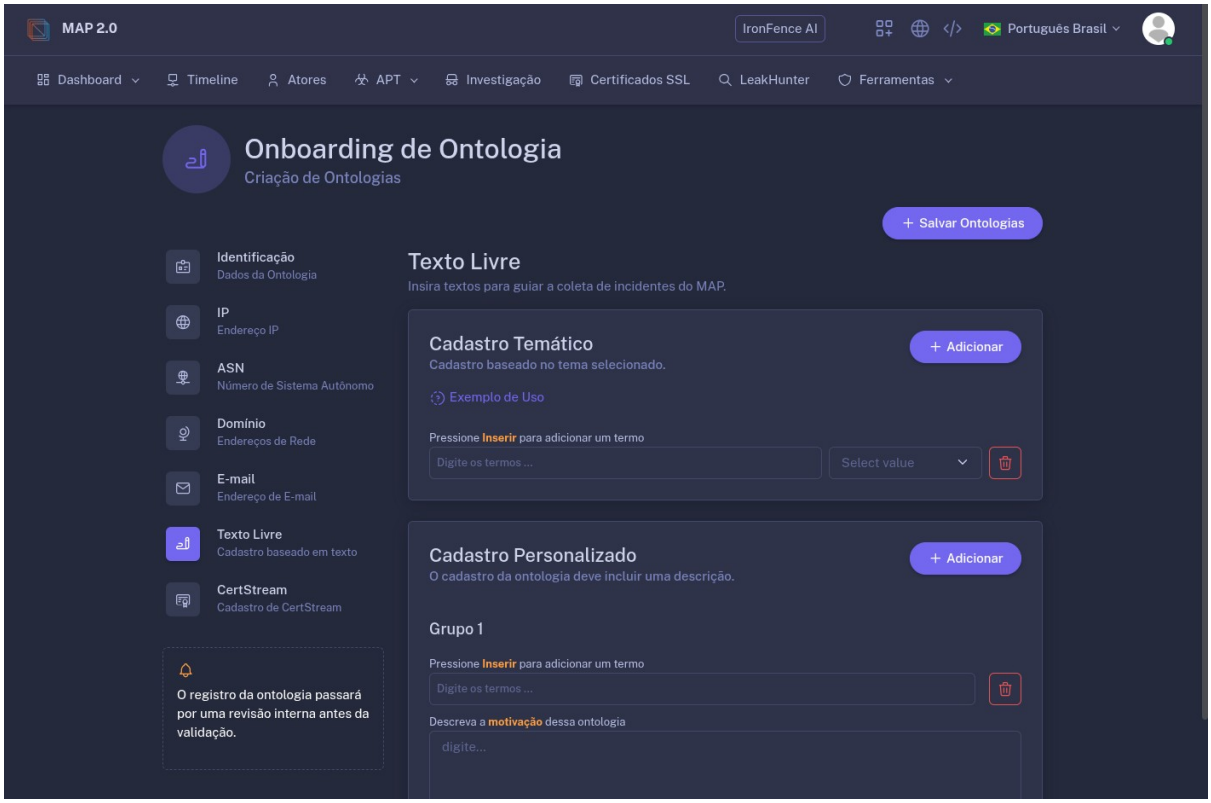
https://apps.dataverso.net/user/create

2.3. Todos os custos envolvidos na prestação dos serviços, tais como: alocação de pessoas, aluguel, energia, computadores, softwares e demais custos serão de inteira responsabilidade da CONTRATADA.

A plataforma IronFence MAP opera integralmente em infraestrutura própria em nuvem privada, não demandando investimentos em hardware, software ou recursos humanos por parte do CONTRATANTE.

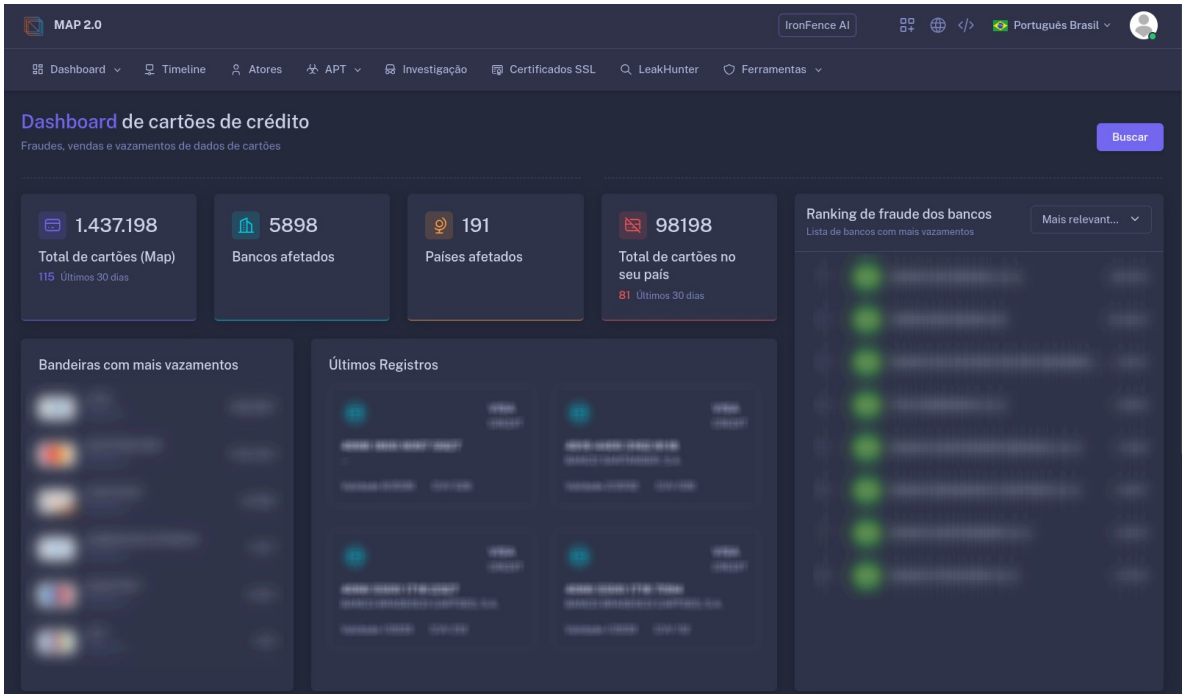
2.4. Além dos ativos de TIC, o serviço deve monitorar e reportar indicativos de uma listagem de serviços de tecnologias e softwares que são utilizadas pelo Banco do Nordeste.

Durante o processo de onboarding do Banco do Nordeste, o MAP realizará a coleta e o levantamento detalhado da infraestrutura e das tecnologias, sistemas, softwares e serviços de TIC utilizados pela instituição. Essas informações serão cadastradas na plataforma para compor a superfície de ataque monitorada, permitindo a identificação proativa de vulnerabilidades, exposições e ameaças associadas ao stack tecnológico do BNB. O monitoramento abrange, entre outros: ASN, domínios, endereços IP, servidores web, frameworks, CMSs, serviços de e-mail, plataformas de nuvem, bibliotecas e componentes de terceiros.



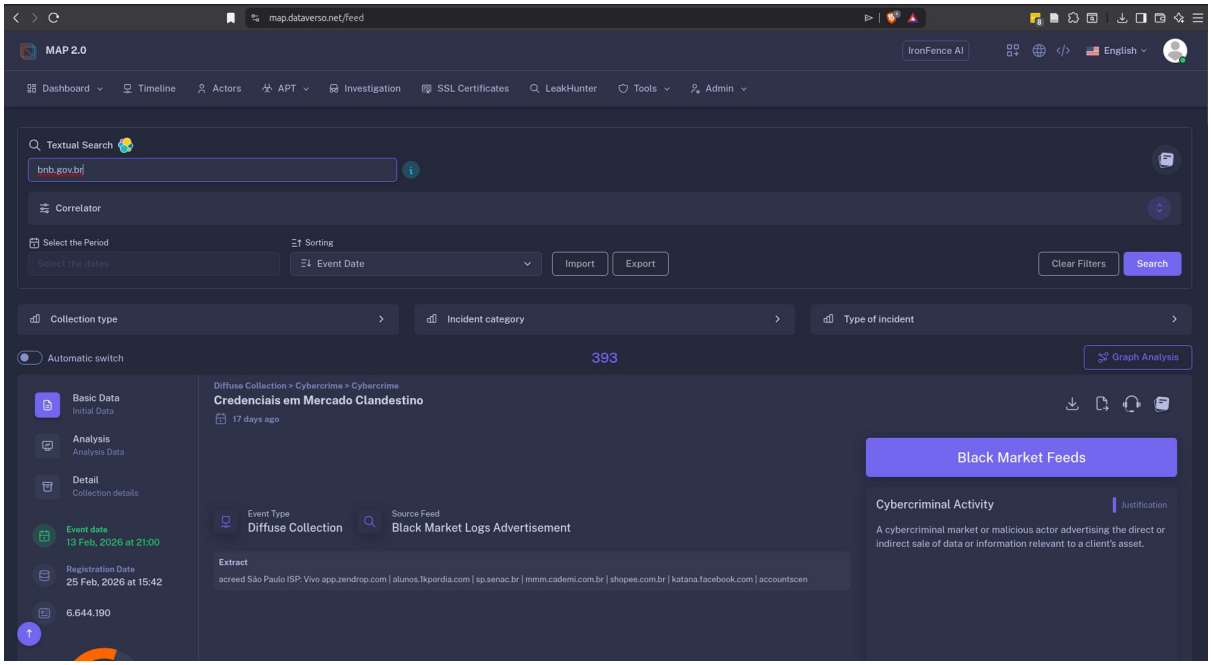
https://map.dataverso.net/admin/onboarding/set-up

2.5. O serviço deve monitorar as BINs de cartões informados pelo Banco, verificando se o padrão corresponde a um número de cartão válido.

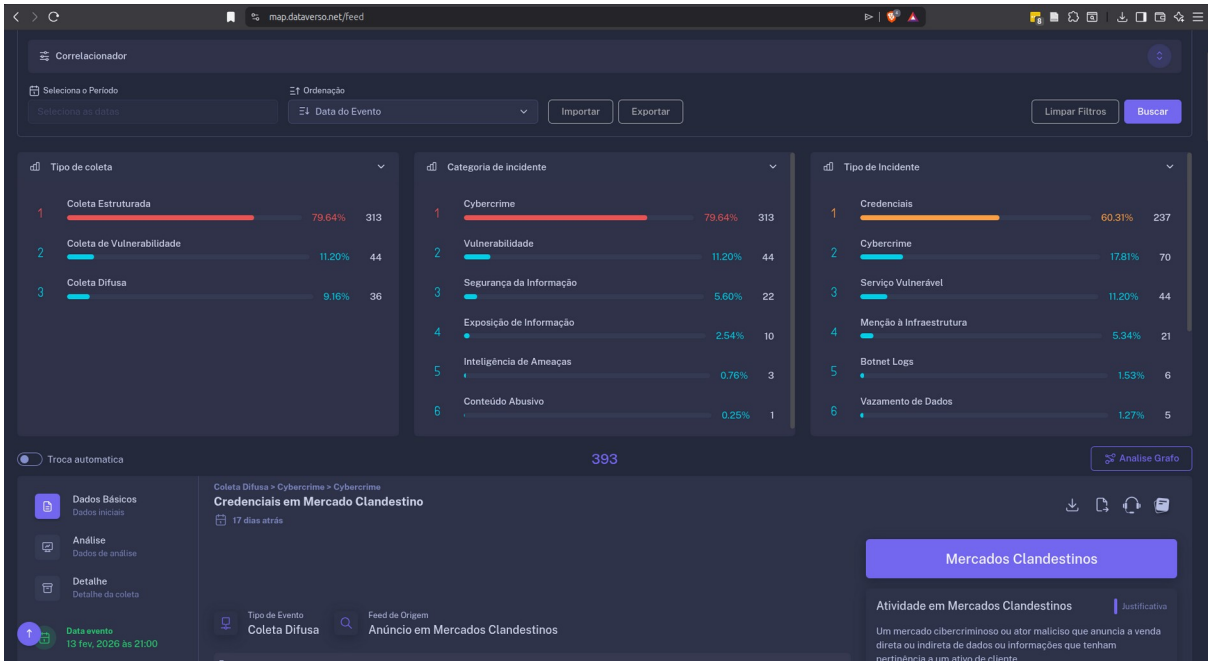


https://map.dataverso.net/dashboard/creditCard

2.6. O serviço deve monitorar e reportar indicativos de ameaças a usuários do domínio @bnb.gov.br, inclusive as credenciais vazadas do Banco.

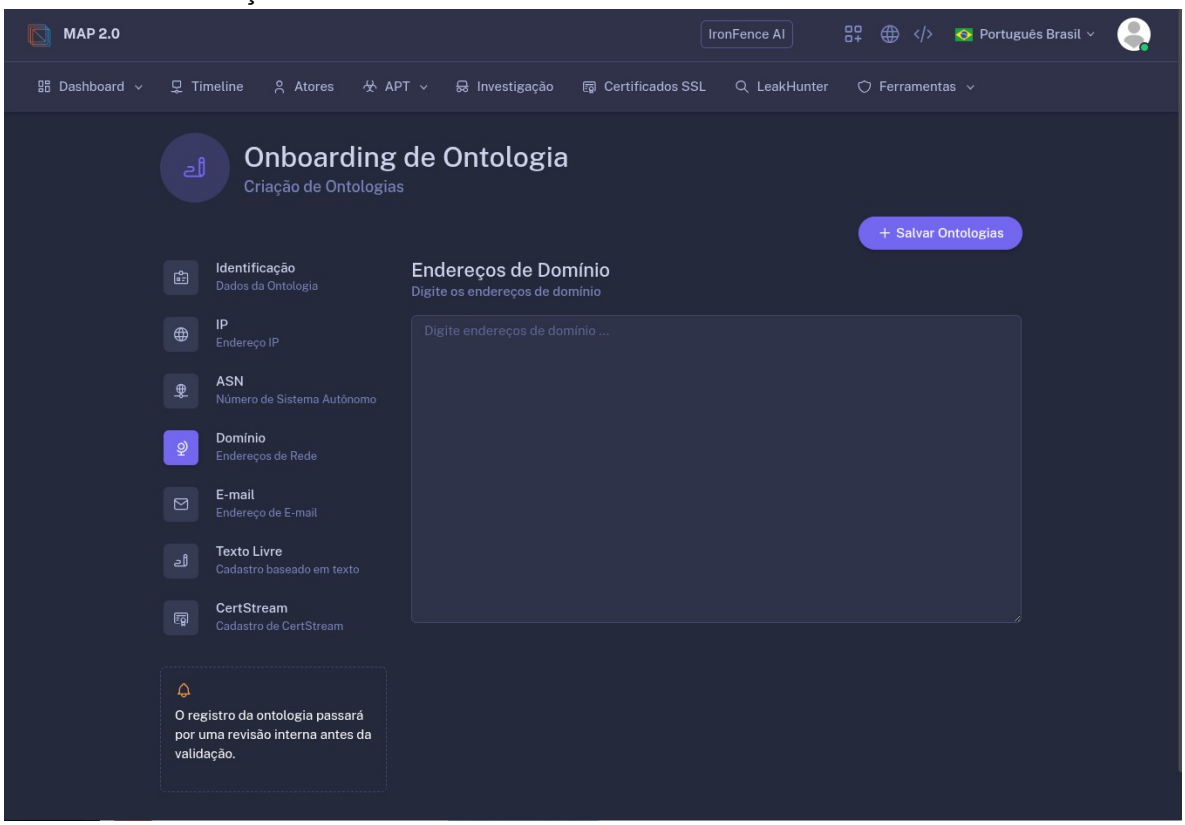


2.7. Para efeito de reporte, o serviço de CTI irá gerar eventos em, pelo menos, 3 categorias:
Eventos de Informação: Estes eventos não requerem qualquer ação. Este grupo de eventos deve ser utilizado quando não há risco cibernético aos ativos de TIC e de informação monitorados, por exemplo, uma menção simples em uma rede social contendo o nome dos ativos de TIC e de informação do CONTRATANTE;
Eventos de Aviso: Este grupo de eventos deve ser utilizado quando existe algum comportamento que represente risco cibernético em relação aos ativos de TIC e de informação monitorados, por exemplo, uma menção na internet, deep ou dark web, ou qualquer outro meio monitorado, com contexto de ameaças e/ou ataques cibernéticos direcionados contra o BNB;
Eventos de Exceção: Estes eventos são aqueles que sugerem que os princípios da PSIBC (confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade, privilégio mínimo, necessidade de conhecer, proteção de dados pessoais e proteção da privacidade), foram impactados negativamente. São exemplos desses eventos: detecção de um vazamento de dados do CONTRATANTE e venda de informações atreladas aos ativos de informação monitorados em canais de fraude.



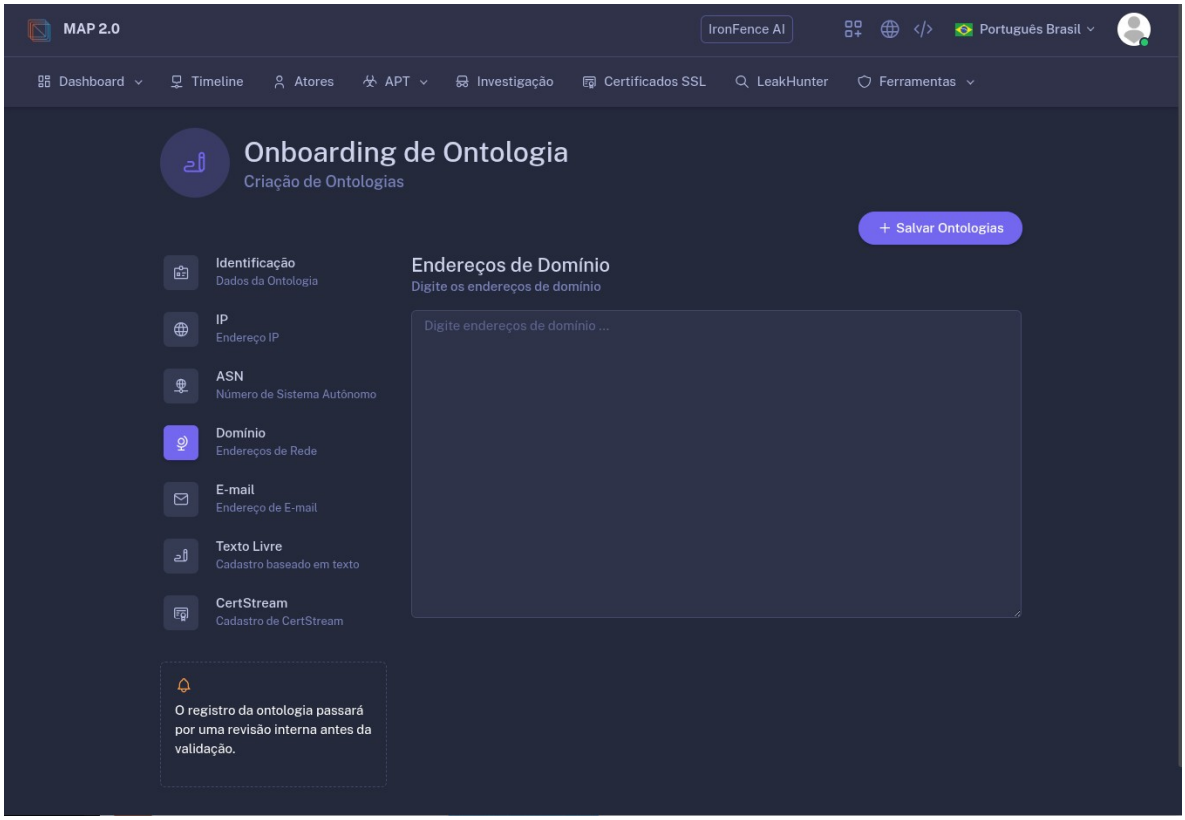
Categorias de incidente customizáveis pelo cliente em https://map.dataverso.net/feed

2.8. O BNB deverá fornecer previamente à CONTRATADA responsável pelo serviço de CTI a lista de ativos de informação a serem monitorados.



https://map.dataverso.net/admin/onboarding/set-up

2.9. A lista de ativos de informação pode ser alterada, caso seja necessário, para atender às demandas de segurança cibernética da instituição, sendo sempre comunicadas à CONTRATADA para devida atualização do monitoramento.



https://map.dataverso.net/admin/onboarding/set-up

2.10. Caso a CONTRATADA identifique a ausência de insumos necessários para a geração dos Eventos, será reponsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo.
O BNB, sempre que solicitado, repassará para a CONTRATADA as informações necessárias para aprimorar este processo.

2.11. O serviço deverá ser acessível, através de API e Console, com as seguintes características:
2.11.1. Devem ser disponibilizados, no mínimo, 10 (dez) usuários com acessos simultâneos;

A plataforma MAP não impõe qualquer limite técnico ao número de sessões simultâneas. O gerenciamento de sessões é feito pelo framework **Laravel** com driver **Redis**, que suporta múltiplas sessões concorrentes sem restrição por design. A capacidade de acessos simultâneos é dimensionada pela infraestrutura em nuvem da CONTRATADA, que garante disponibilidade para o número de usuários contratados.

2.11.2. Deve ter a autenticação integrada com Microsoft Entra ID (Antigo Azure AD) do BNB.

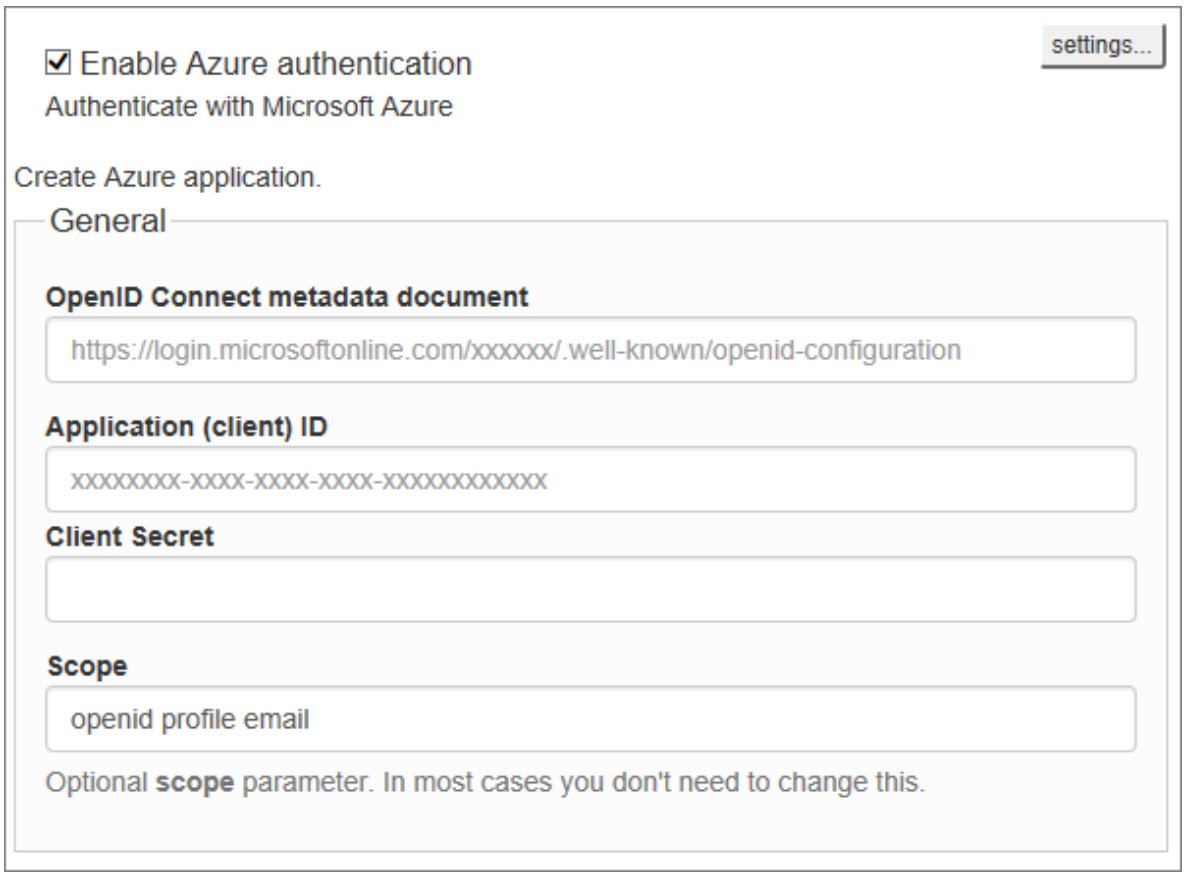
A plataforma de análise do MAP, desenvolvida em **Laravel/PHP**, implementa autenticação federada com o Microsoft Entra ID por meio do pacote oficial **Laravel Socialite** (`laravel/socialite`) em conjunto com o provider `socialiteproviders/microsoft-azure`, utilizando o protocolo **OAuth 2.0 / OpenID Connect**, que é o protocolo nativo e homologado pelo Microsoft Entra ID.

A integração permite que usuários do domínio `@bnb.gov.br` realizem login na plataforma MAP por meio do fluxo SSO corporativo do BNB, sem necessidade de credenciais separadas, bastando configurar o `tenant_id` e as credenciais de aplicativo Azure (`client_id` e `client_secret`) fornecidas pelo BNB.

A configuração da autenticação integrada com o Microsoft Entra ID do BNB requer que o BNB forneça à IronFence as seguintes informações do seu tenant Azure AD: `tenant_id`, `client_id` e `client_secret` de um aplicativo registrado no Entra ID com permissão de autenticação. Tais informações são necessárias para que a IronFence configure o ambiente no MAP. Portanto, não é só uma questão técnica da IronFence - é uma ação administrativa que depende também do BNB para a efetiva integração.

Referências técnicas (documentação oficial dos fabricantes):

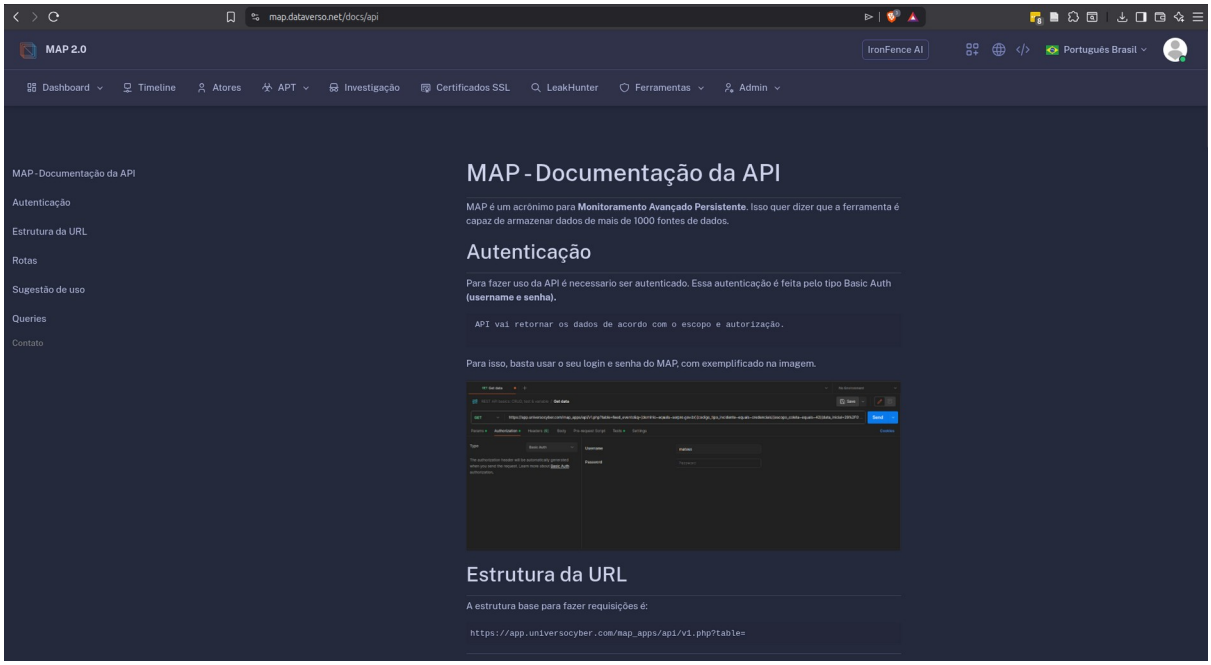
- Laravel Socialite — autenticação OAuth com provedores externos: https://laravel.com/docs/socialite
- Provider Microsoft Azure para Laravel Socialite: https://socialiteproviders.com/Microsoft-Azure/
- Protocolo OAuth 2.0 / OpenID Connect do Microsoft Entra ID: https://learn.microsoft.com/en-us/entra/identity-platform/v2-oauth2-auth-code-flow



Configuração da autenticação federada com o Microsoft (Ativação sob demanda pelo time de desenvolvimento do MAP)

2.11.3. Não deve ser instalado na infraestrutura de TIC do BNB;

https://map.dataverso.net/dashboard e https://map.dataverso.net/docs/api

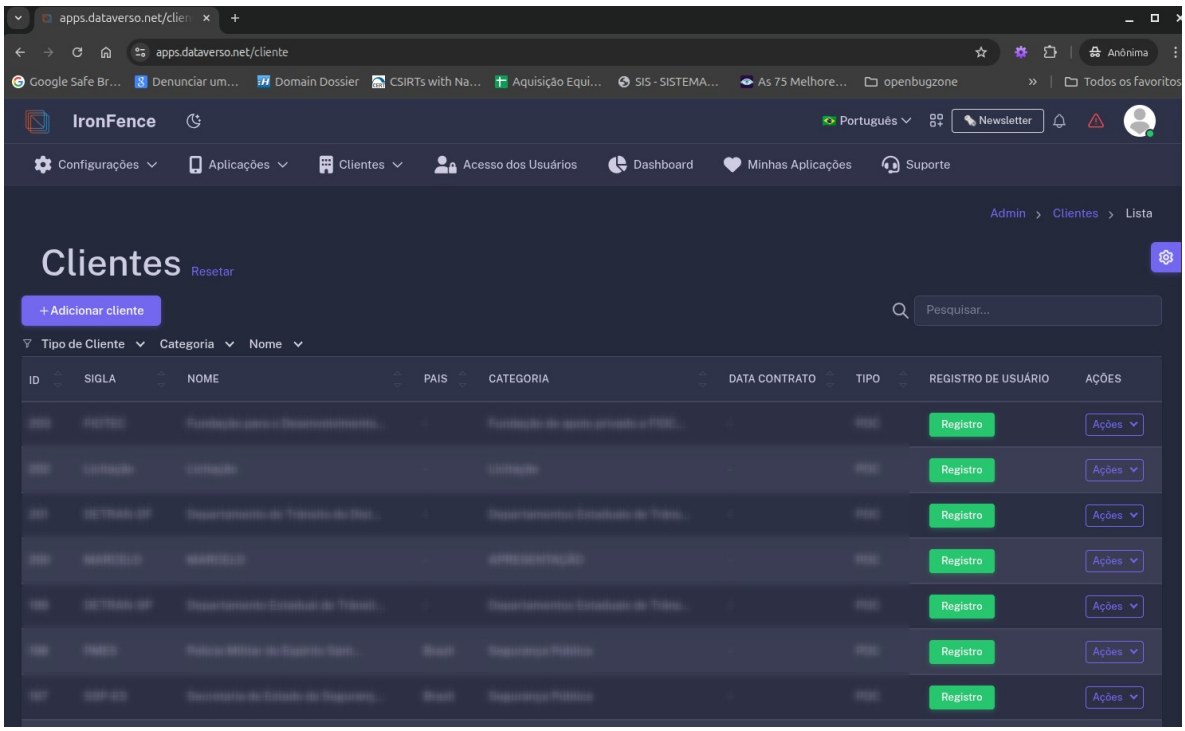


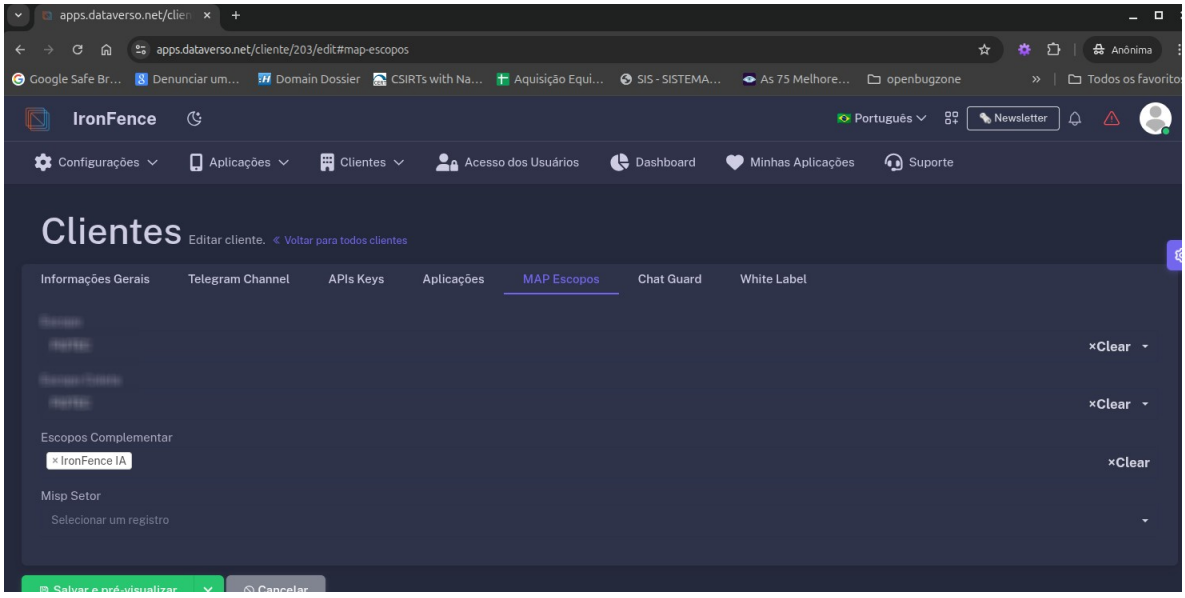
2.12. O serviço deverá disponibilizar a console via interface web, por meio de URL segura (HTTPS), TLS v 1.2 e cifras fortes além de configuração de HSTS.

https://map.dataverso.net/dashboard

2.13. Da Confidencialidade, Integridade e Disponibilidade dos dados de CTI, a CONTRATADA deverá:
2.13.1. Implementar os controles necessários para que apenas os seus profissionais, bem como os usuários e grupos criados por esta instituição, tenham acesso às pesquisas realizadas e aos dados armazenados;

A plataforma MAP implementa isolamento de dados por cliente através de arquitetura **multi-tenant**, onde cada contratante acessa exclusivamente seus próprios dados e pesquisas. O controle de acesso é implementado via sistema de **roles e permissões** do Laravel, garantindo que apenas os profissionais da CONTRATADA e os usuários criados pelo BNB tenham acesso às informações do BNB.



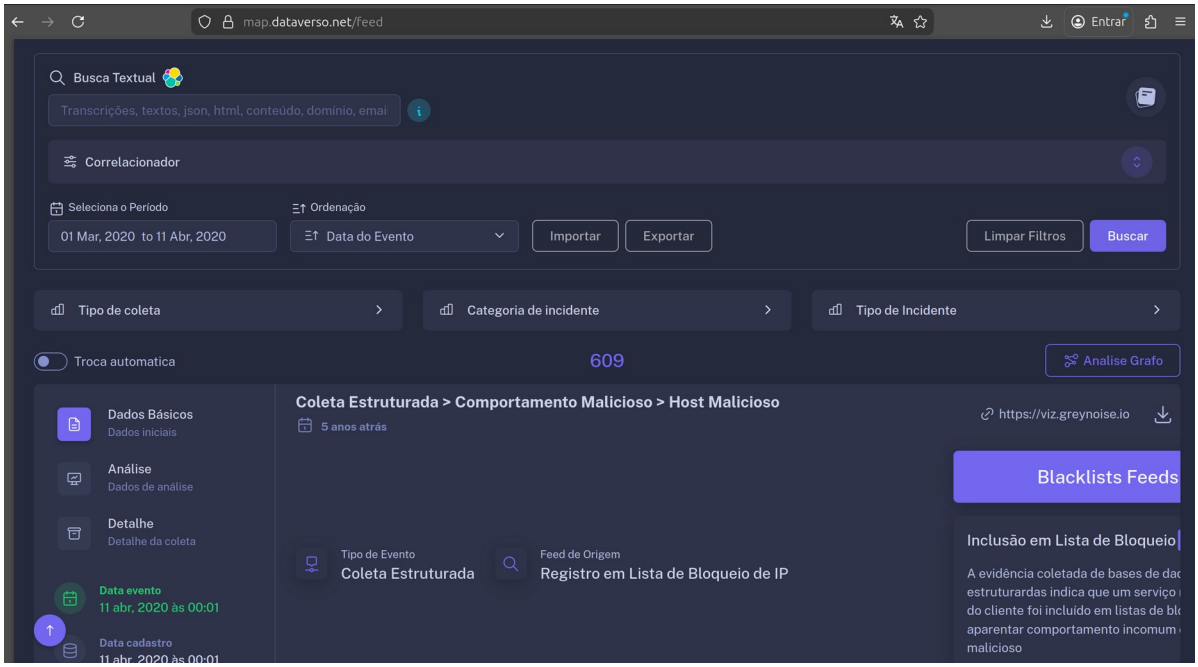


Para cada cliente é possível definir um ou mais escopos específicos.

2.13.2. Se responsabilizar pela guarda das informações coletadas por período a ser definido pelo BNB, não menor que 12 (doze) meses;

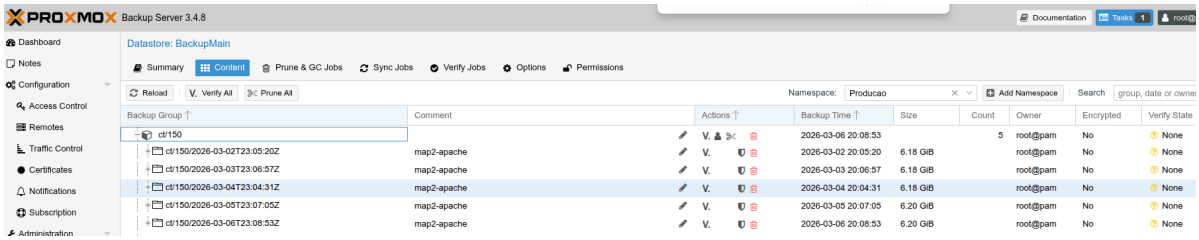
A CONTRATADA se compromete contratualmente à guarda das informações coletadas pelo período definido pelo BNB, não inferior a 12 meses. Tecnicamente, a plataforma retem as coletas bem superior ao requisito do BNB, coforme imagem abaixo pode ser observado no print indicando

um evento de 5 anos atrás.



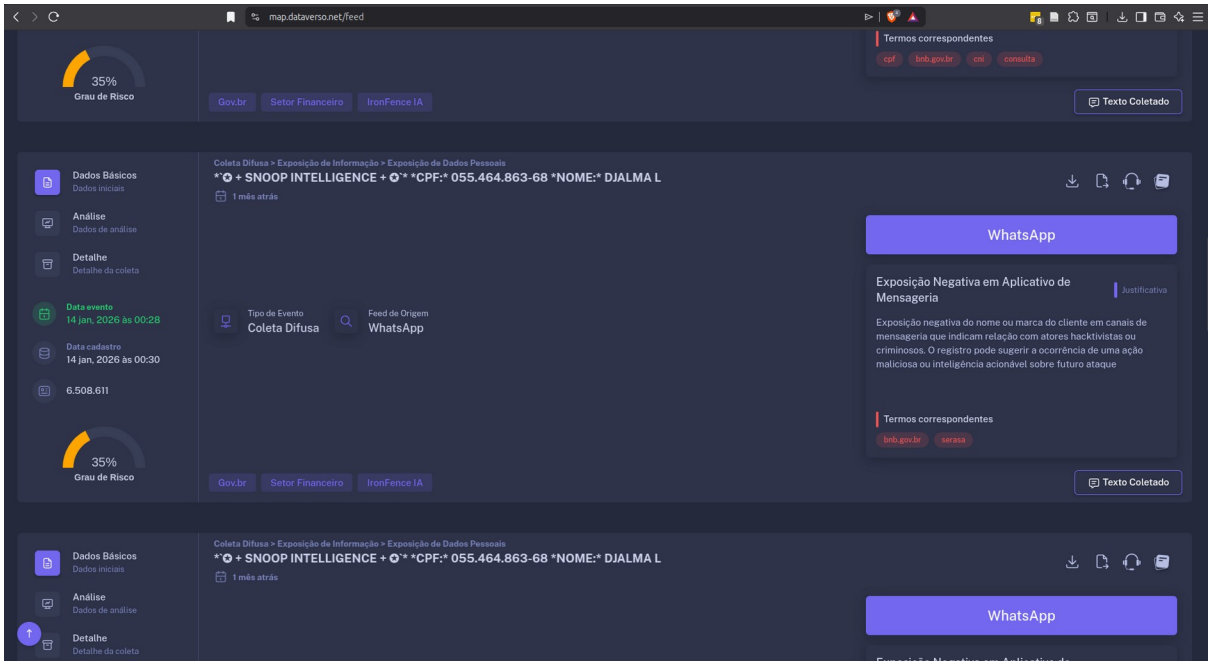
2.13.3. Realizar cópia de segurança dos dados coletados em razão dos ativos de informação monitorados, de forma a permitir ao menos a restauração das pesquisas realizadas e de seus resultados. Observação: Essas informações, quando solicitadas pelo BNB, devem ser repassadas nos formatos HTML, PDF, CSV, Planilha eletrônica e DOCX.

Backup: A plataforma MAP opera em infraestrutura virtualizada com **Proxmox VE**, e as cópias de segurança são realizadas de forma automatizada pelo **Proxmox Backup Server (PBS)**, que executa backups incrementais das máquinas virtuais em intervalos regulares, garantindo a possibilidade de restauração completa das pesquisas realizadas e de seus resultados. O PBS permite restauração granular de dados, assegurando a recuperação das informações coletadas em razão dos ativos monitorados do BNB.



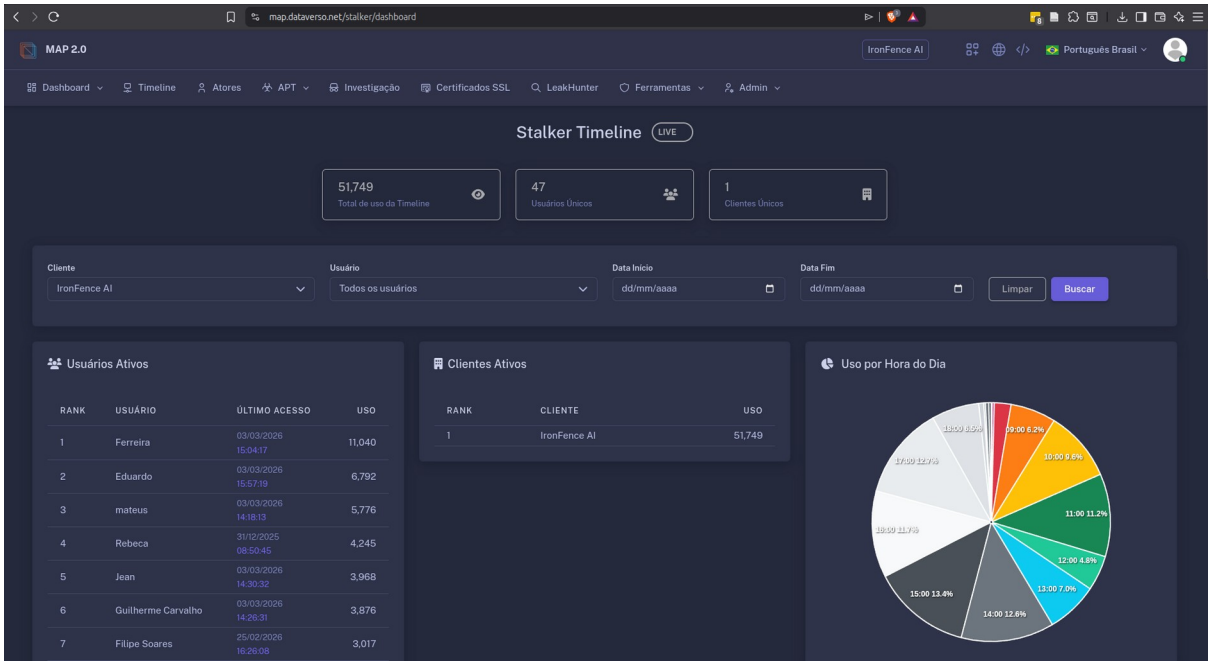
https://apps.dataverso.net/

2.13.4. Disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, contexto, metadados e tipo da fonte.



https://map.dataverso.net/feed

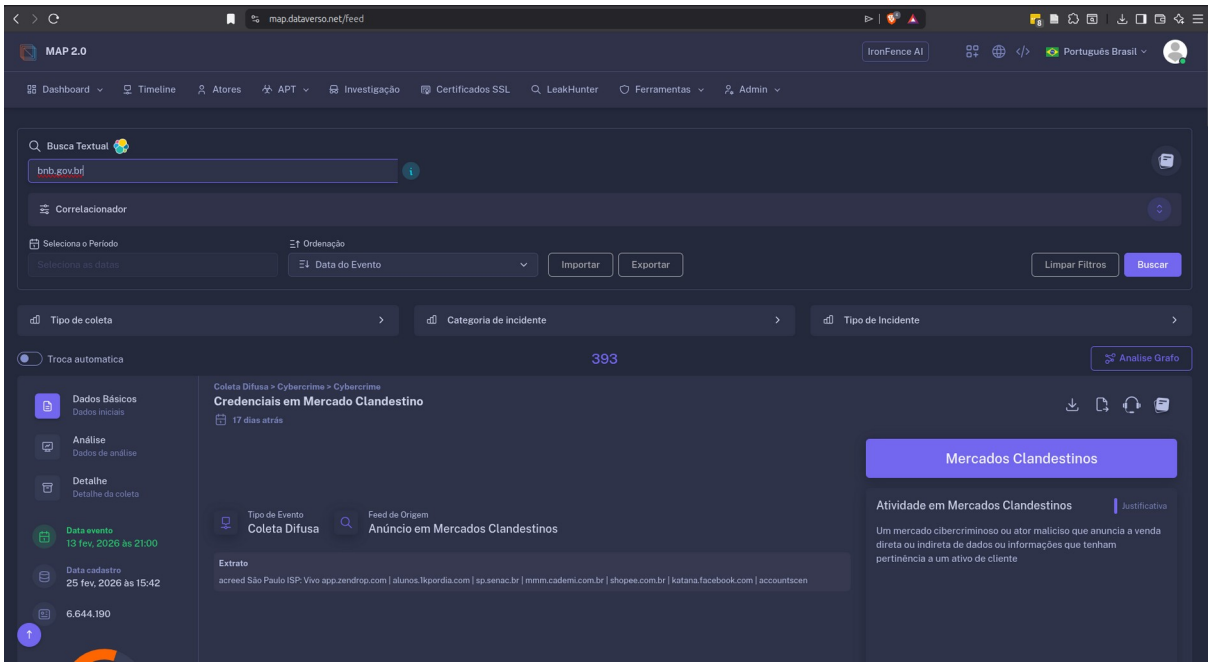
2.13.5. Gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todas as contas de usuários. Os registros de logs devem conter, no mínimo, a data e hora do evento, origem de acesso, usuário, hostname do equipamento e ação/pesquisa efetuada.



https://map.dataverso.net/stalker/dashboard

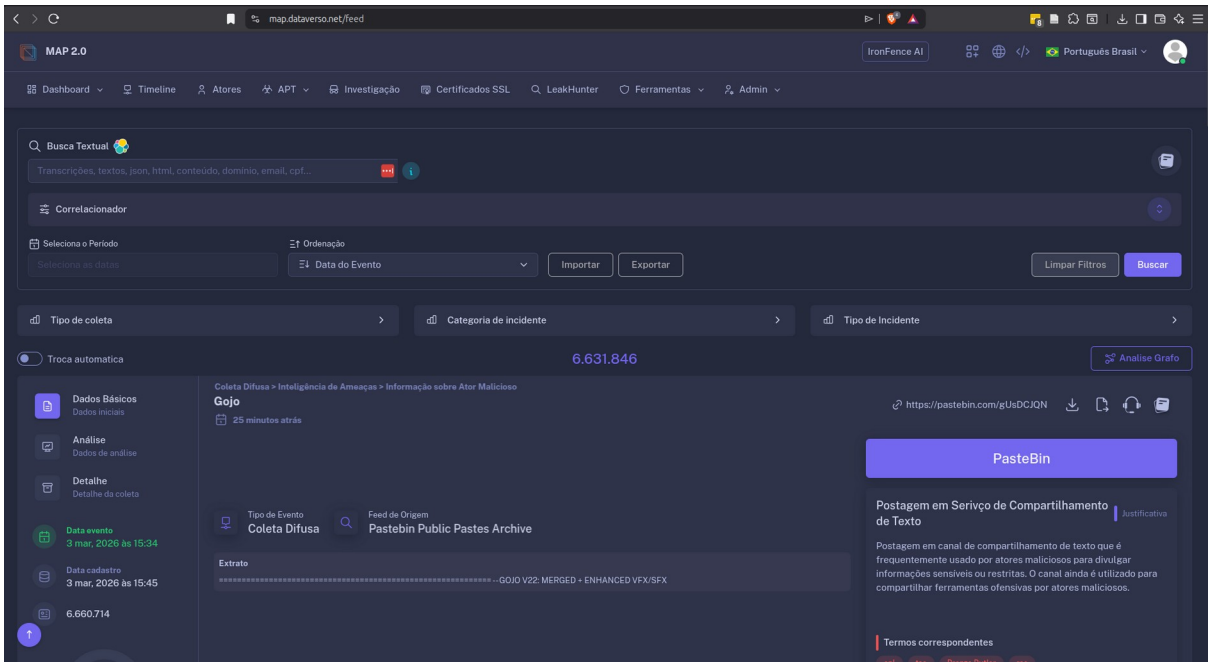
3. SOBRE A CONSOLE DO CTI

3.1. Não limitar quantidade de recursos pesquisados;

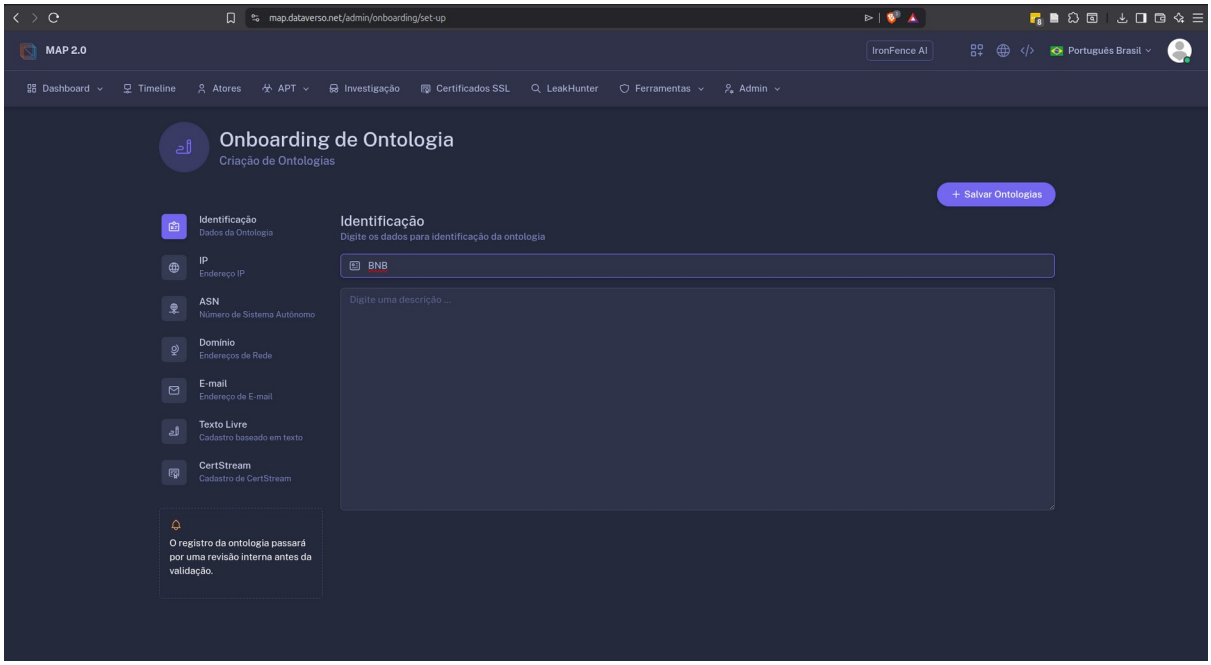


https://map.dataverso.net/feed

393 resultados atualmente identificados do BNB, sendo possível, visualizar 6.631.846

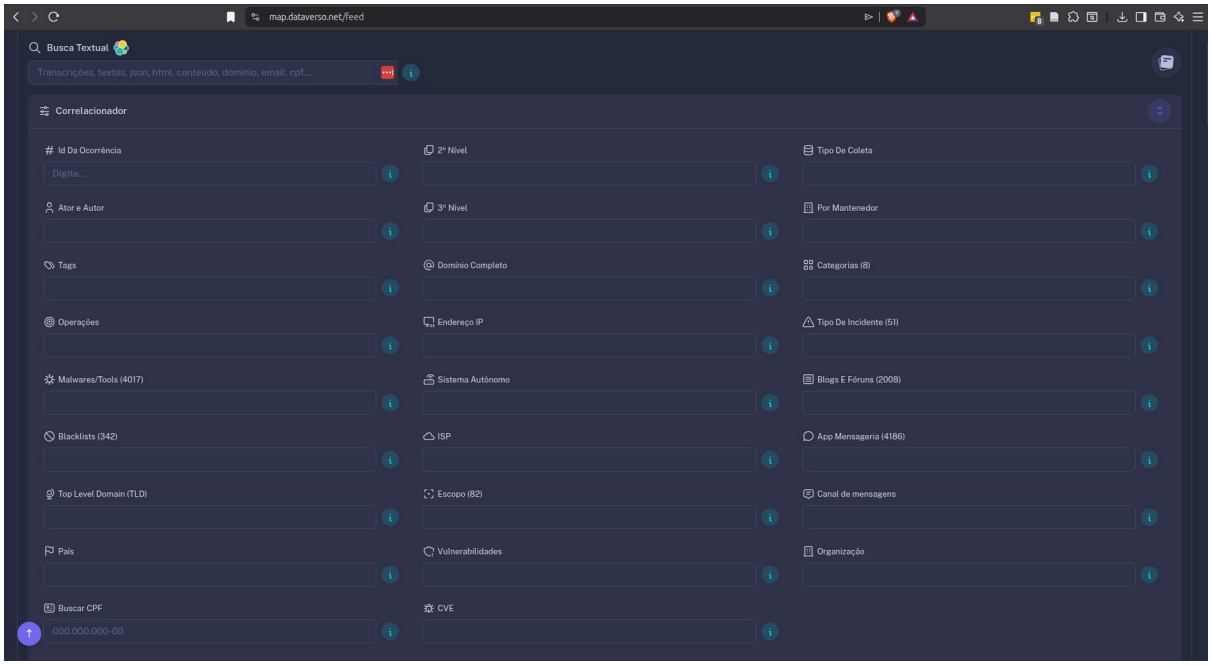


3.2. Prover pesquisa direcionada através da monitoração de palavras pré-selecionadas fornecidas;



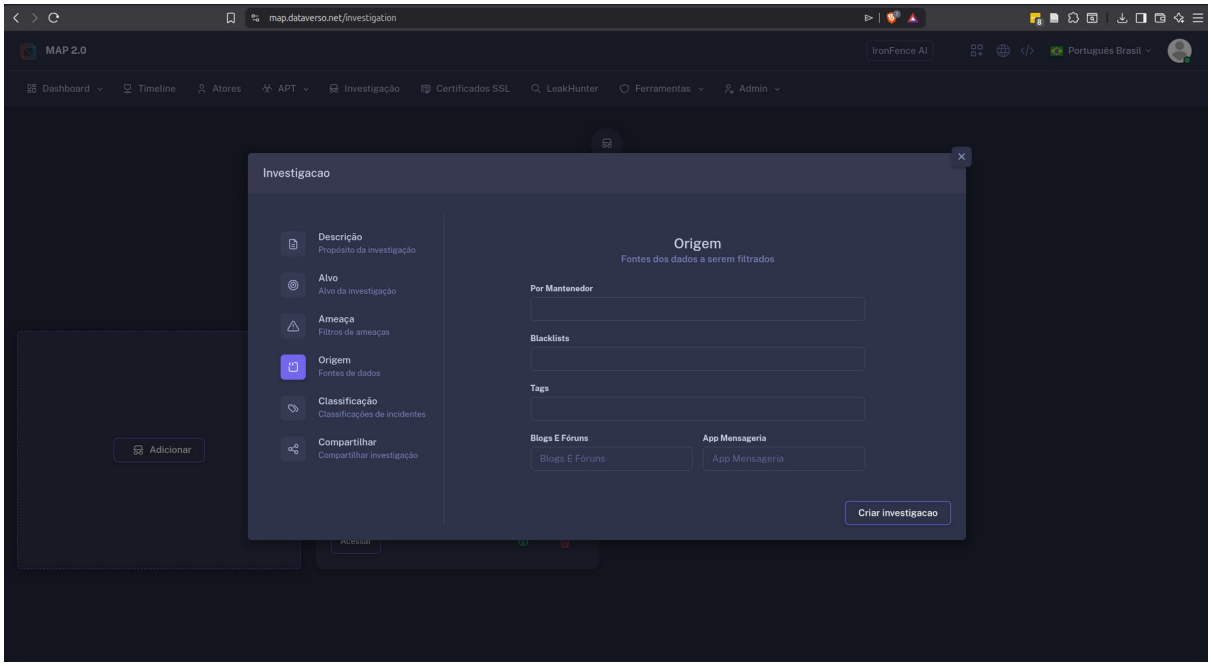
https://map.dataverso.net/admin/onboarding/set-up

3.3. Possuir modelos de filtro de informações pré-configurados, personalizados de acordo com comportamentos conhecidos dos usuários na utilização das diferentes fontes de informação monitoradas.



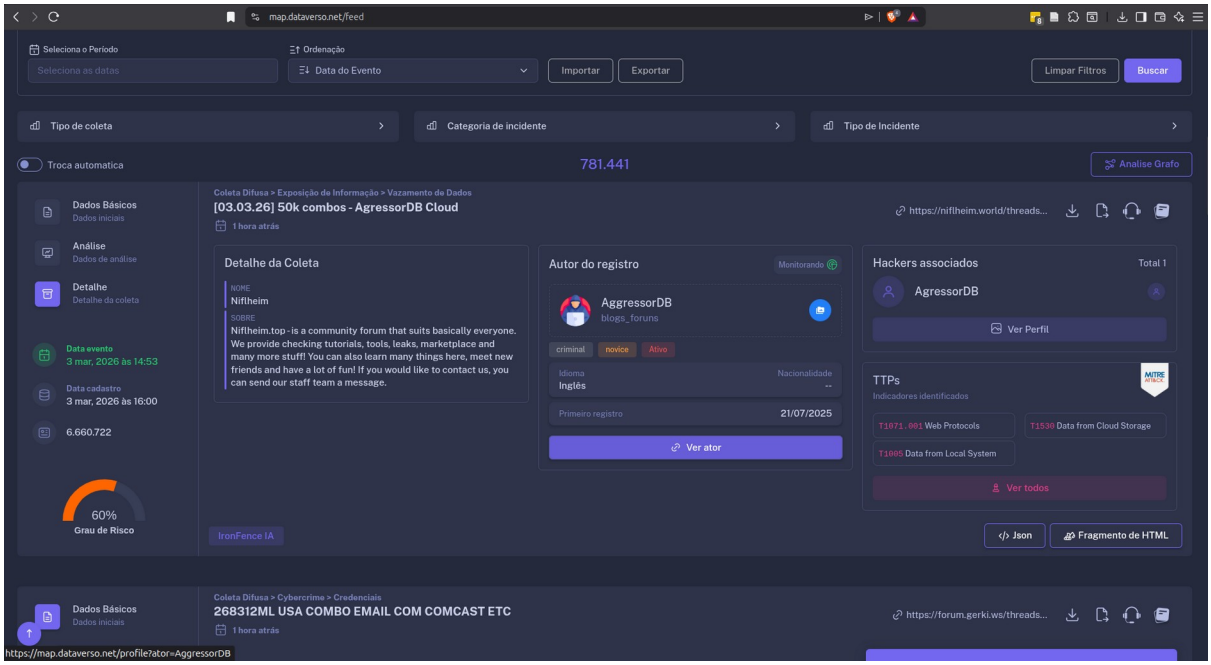
https://map.dataverso.net/feed

3.4. Possibilitar salvar os resultados das pesquisas já realizadas e apresentar os dados filtrados em painéis com as principais fontes identificadas na busca.



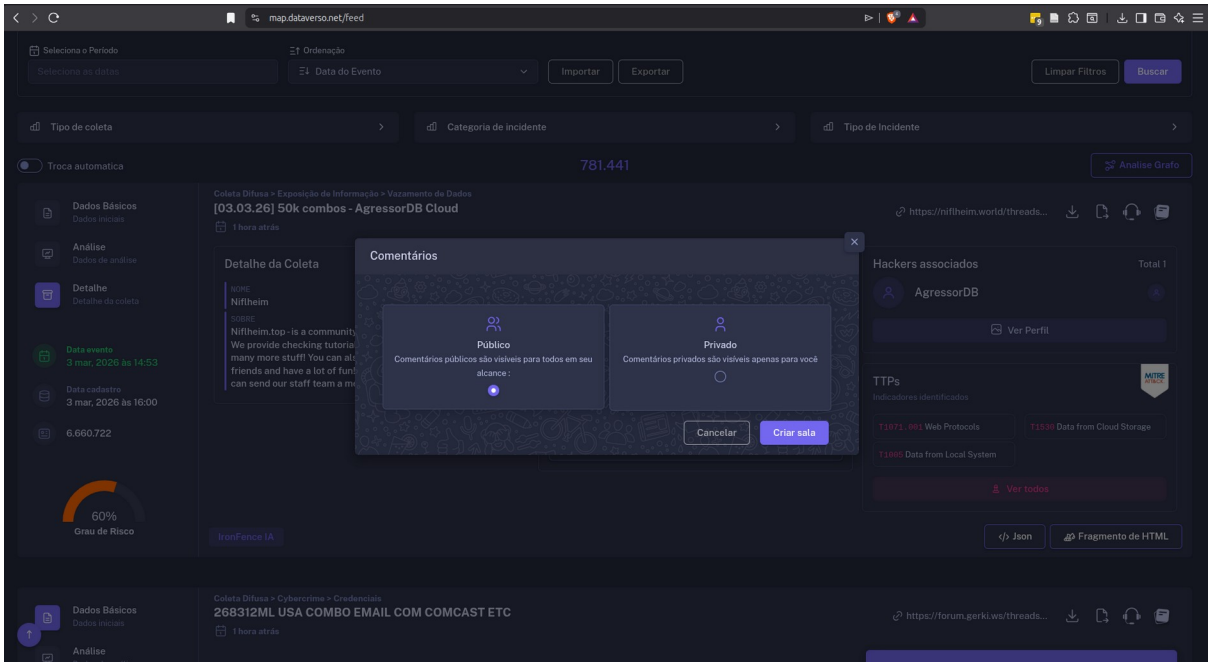
https://map.dataverso.net/investigation

3.5. Permitir a navegação com clicks nos tipos de informações de interesse do painel, com apresentação das informações relacionadas.



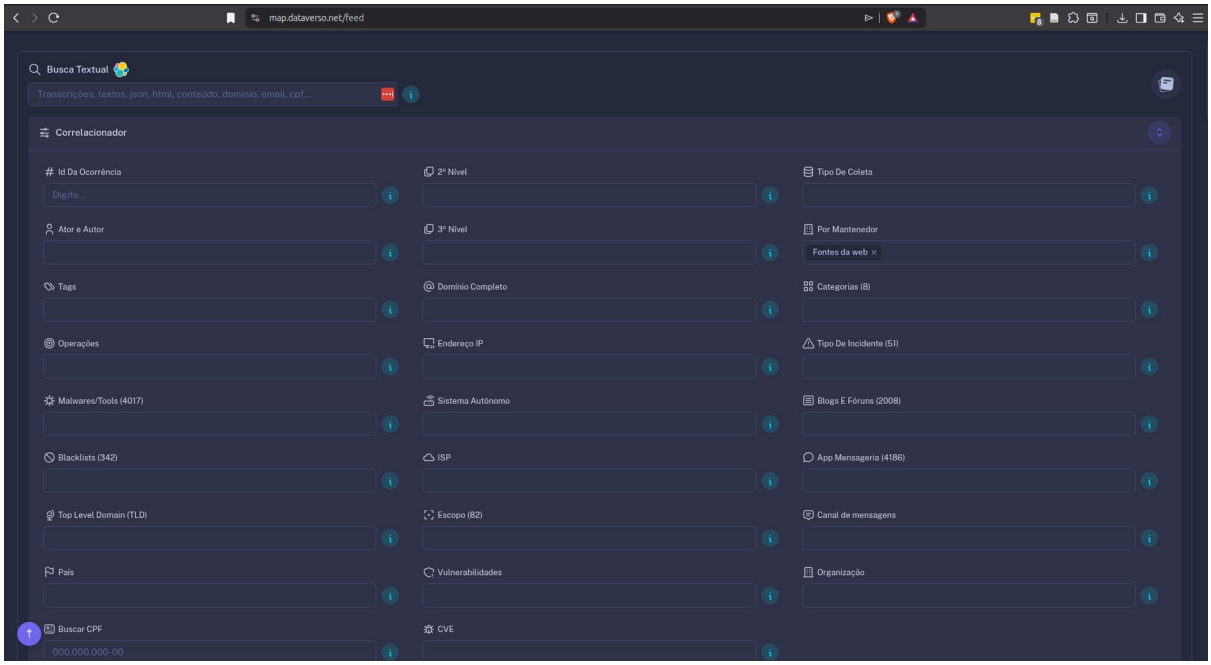
https://map.dataverso.net/feed -> clique em ator para ver perfil específico

3.6. Prover um campo de descrição em que os analistas de segurança cibernética do BNB, ou da CONTRATADA, possam contextualizar as informações associadas aos eventos. Este recurso deve facilitar o consumo das informações de CTI pelas equipes de segurança cibernética, a exemplo das equipes do serviço de CSOC;



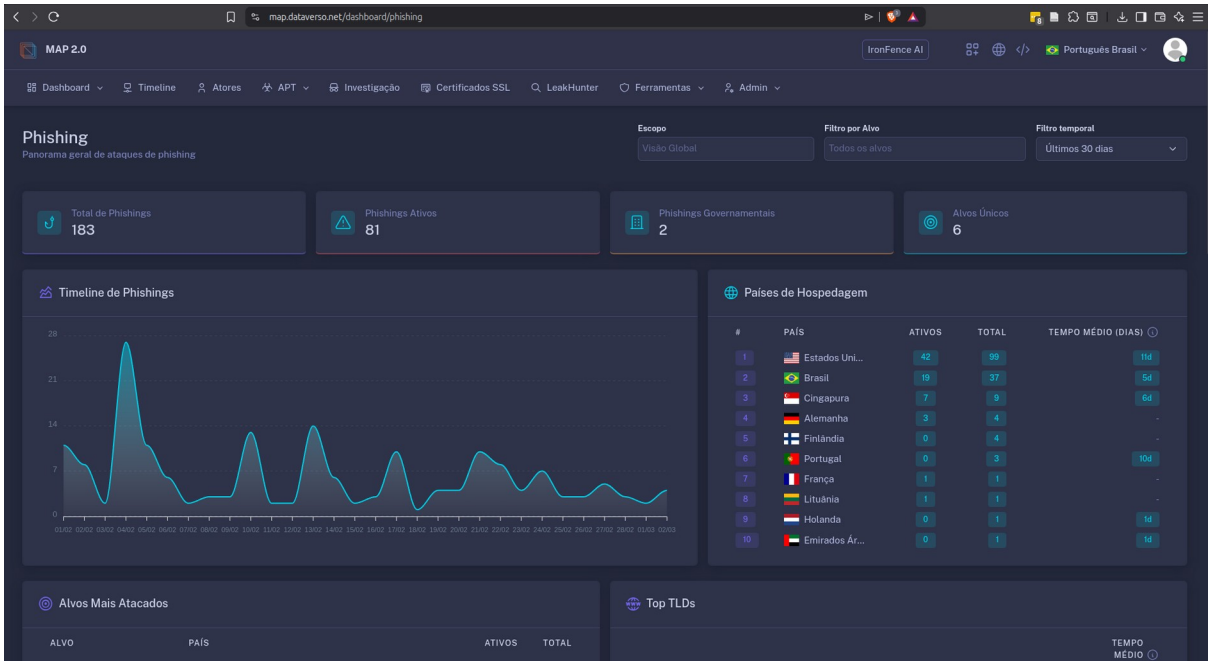
https://map.dataverso.net/feed - comentário no botão de topo à direita de cada incidente

3.7. Permitir a pesquisa de informações nos seguintes contextos:
3.7.1. Ameaças cibernéticas;
3.7.2. Resposta a incidentes;
3.7.3. Prevenção de perdas de dados;
3.7.4. Proteção de Marca e Executivos;
3.7.5. Risco de Terceiros;
3.7.6. Fraude;
3.7.7. Quaisquer outras fontes disponíveis, ou que venham a se tornar disponíveis.



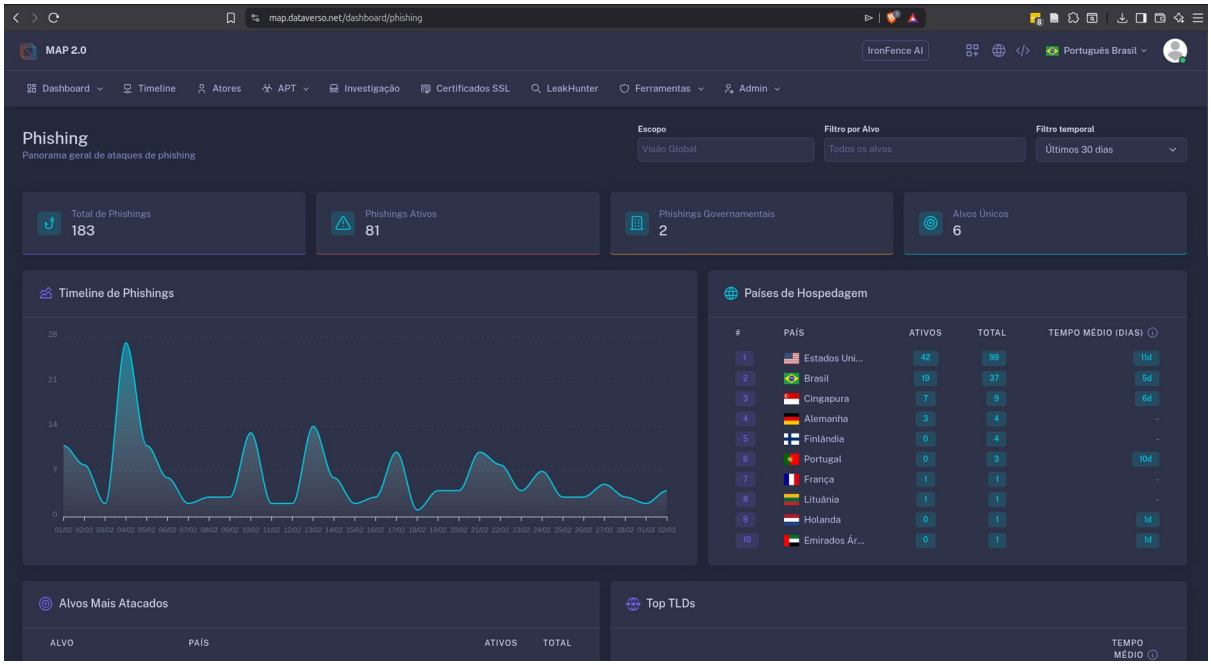
https://map.dataverso.net/feed - clique em correlacionador

3.8. Apresentar a descoberta de páginas web de “phishing”, utilizando o nome dos recursos pesquisados, a marca, identidade visual, domínios e ativos de informação que serão protegidas;



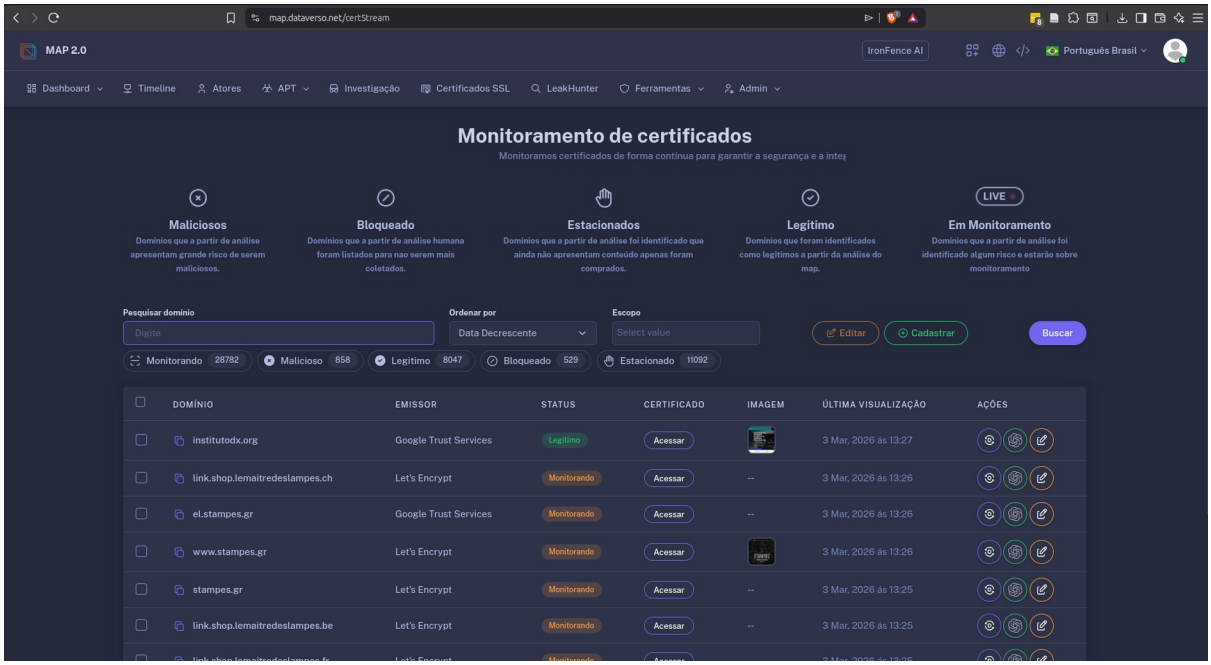
https://map.dataverso.net/dashboard/phishing

3.9. Apresentar a verificação de sites suspeitos de phishing para domínios solicitados pelo CONTRATANTE, ou que tenham sido levantados pela CONTRATADA. Para essa verificação deve-se utilizar, entre outras, as seguintes entidades reguladoras: ICANN (Internet Corporation for Assigned Names and Numbers) e Registro.Br (Registro de Domínios para a Internet do Brasil);



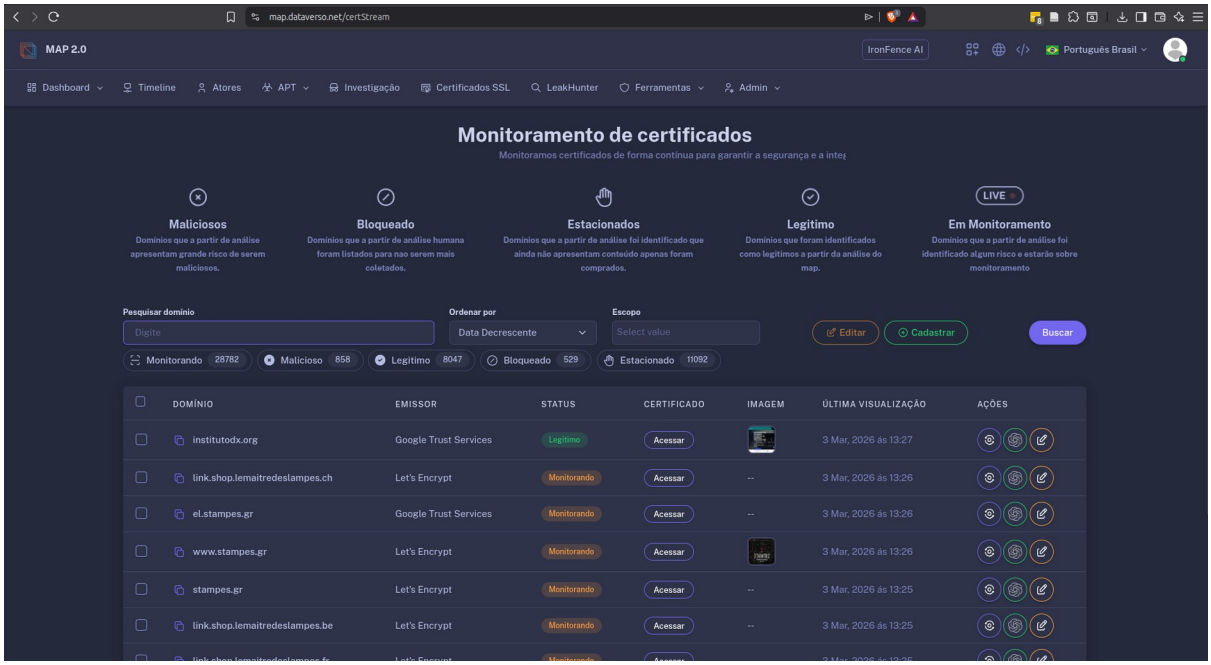
https://map.dataverso.net/dashboard/phishing ,

3.10. Apresentar a detecção de domínios recentemente registrados que possam oferecer riscos e serem utilizados de forma maliciosa contra o BNB como, por exemplo:
3.10.1. Variações comuns de nomes;
3.10.2. Permutações de caracteres; e
3.10.3. Desvio de URL (typosquatting);
3.10.4. Domínios exatos em diferentes TLDs.



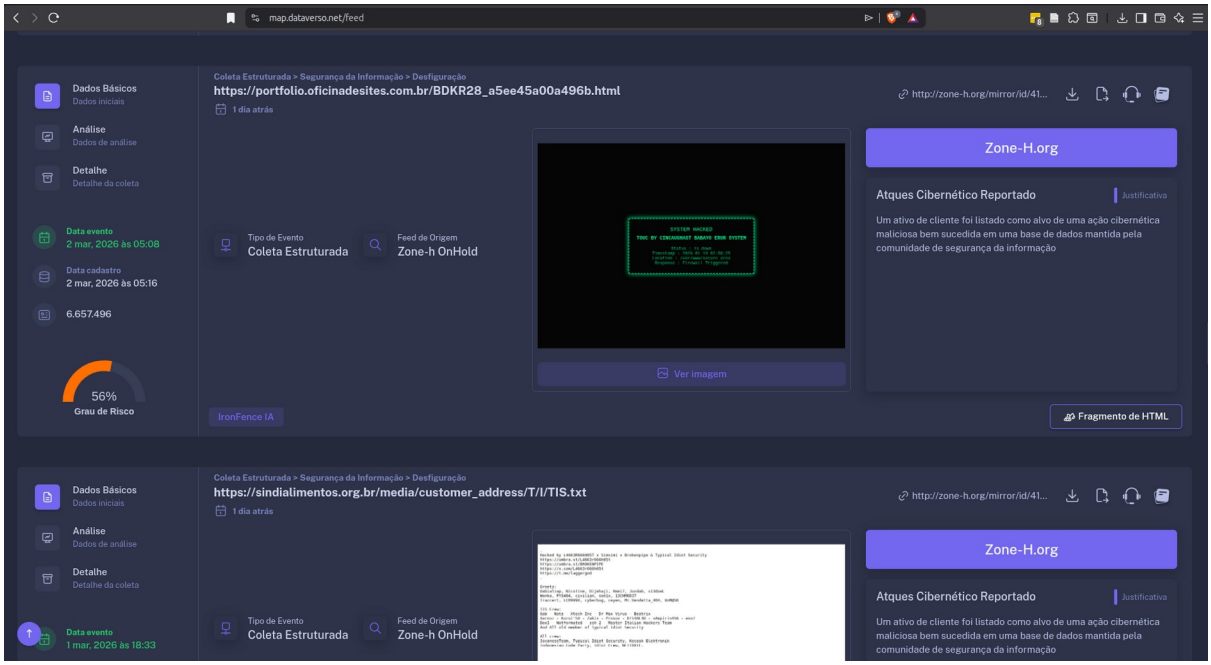
https://map.dataverso.net/certStream

3.11. Nos domínios monitorados a solução deve:
3.11.1. Identificar a emissão de certificados;
3.11.2. Identificar a criação de domínios de recursos monitorados;



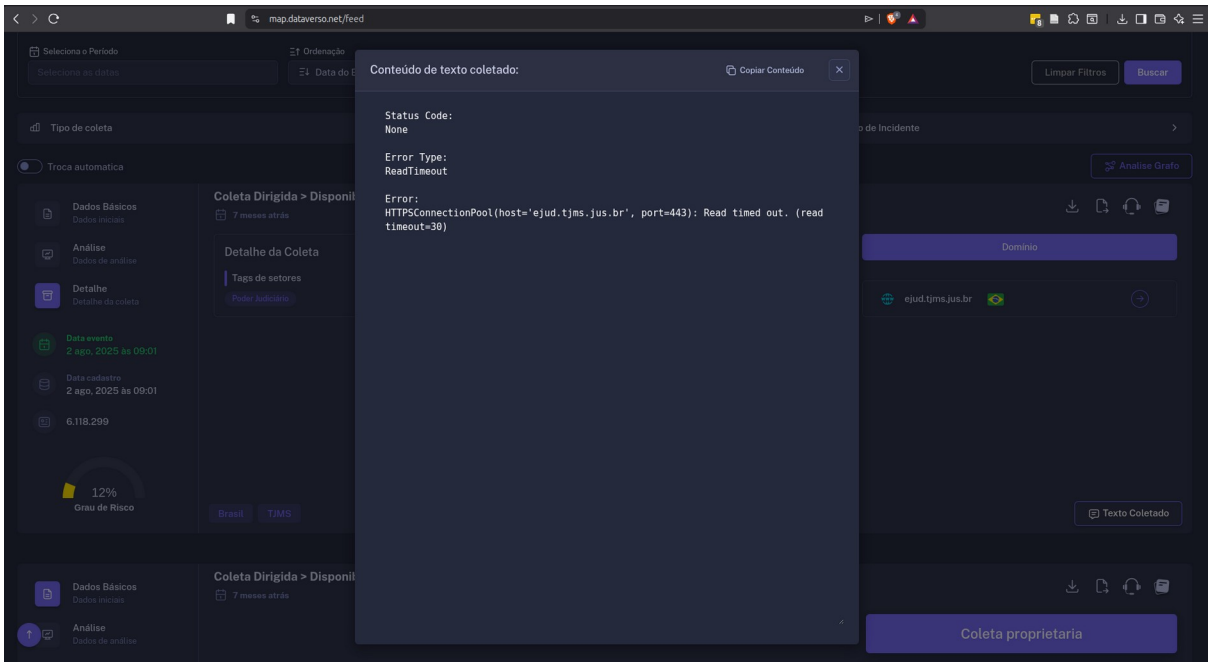
https://map.dataverso.net/certStream

3.12. Identificar a desfiguração de sítio (detecção via código-fonte ou OCR);



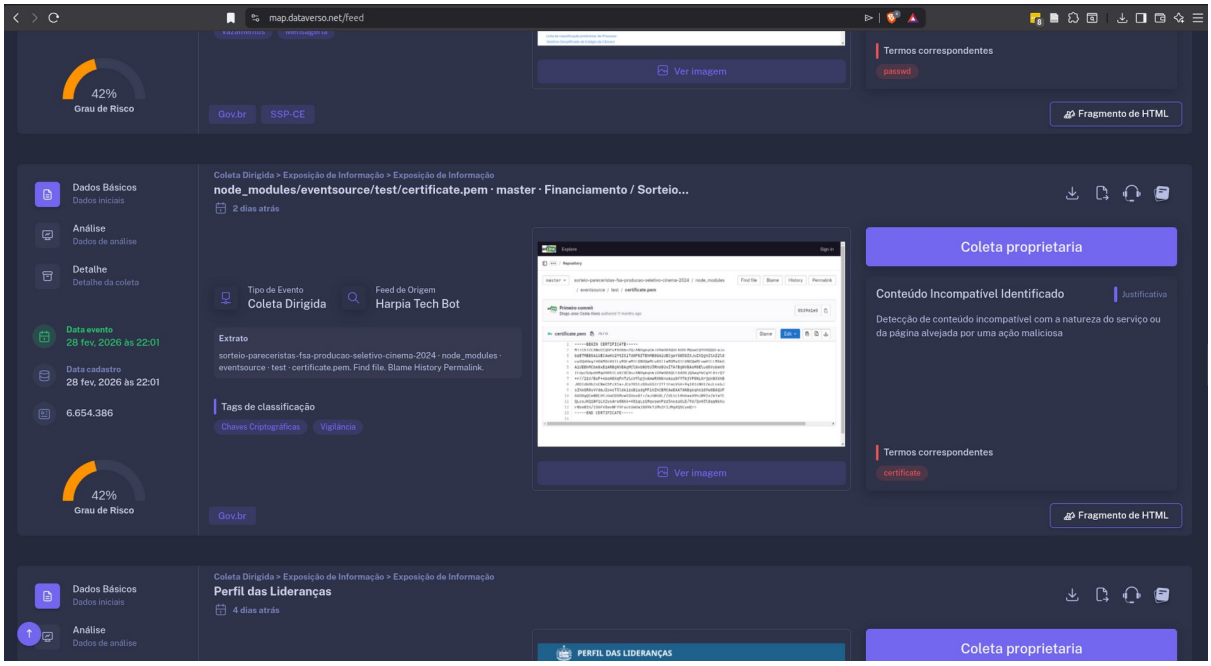
https://map.dataverso.net/feed

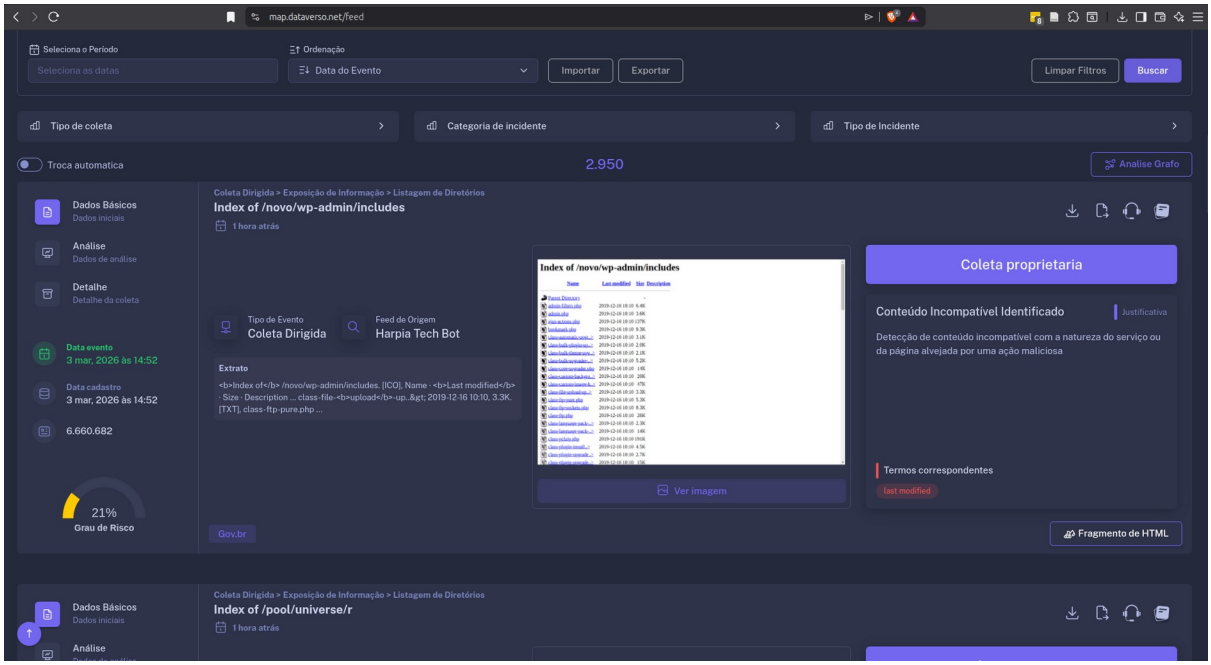
3.13. Identificar a indisponibilidade de domínios (>5 min);



https://map.dataverso.net/feed - serviço indisponível

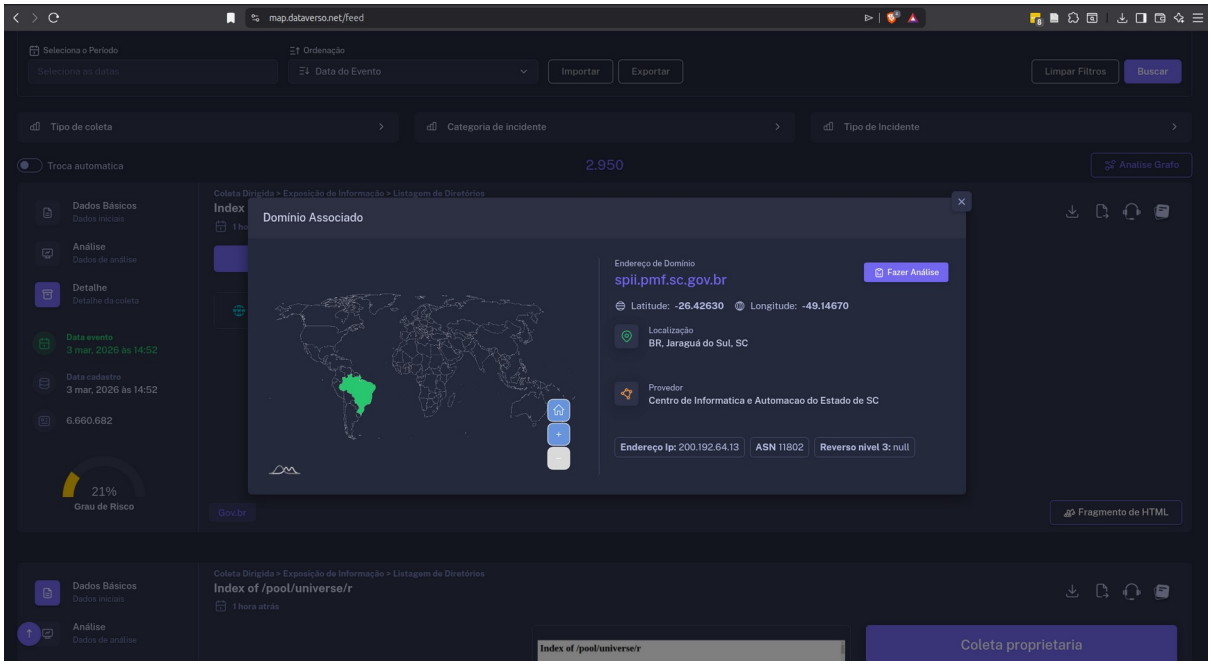
3.14. Identificar diretórios sensíveis e possíveis exposições de dados;





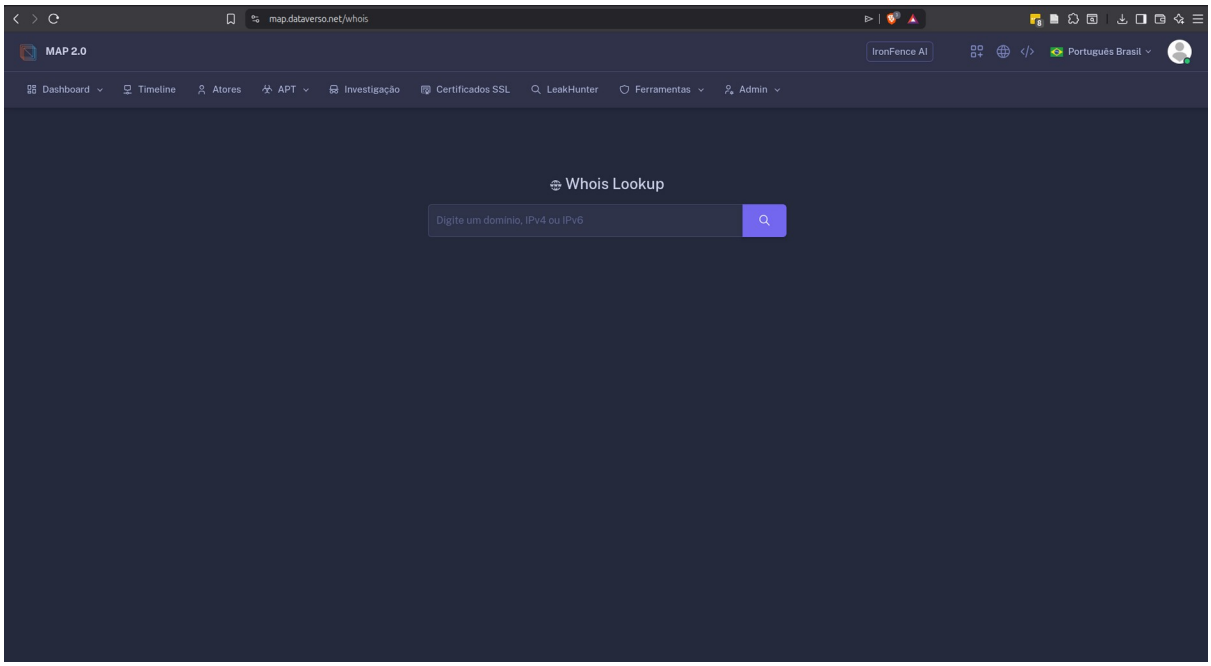
https://map.dataverso.net/feed - tipos de incidente listagem de diretórios e exposição de informação

3.15. Identificar anomalias no registro de URL, timestamp, categoria, snapshot e código-fonte;



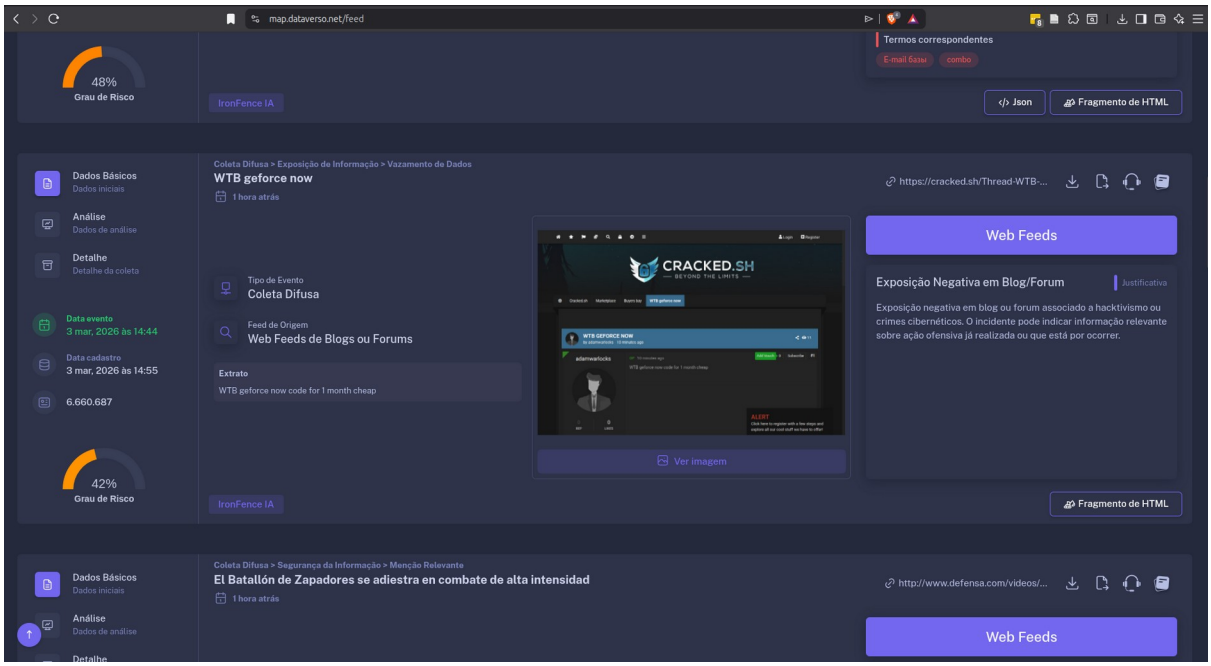
Clicar em detalhes e seta ao lado domínio

3.16. A solução deve realizar consulta Whois de forma automática nos Bots que realizam coletas de domínios.

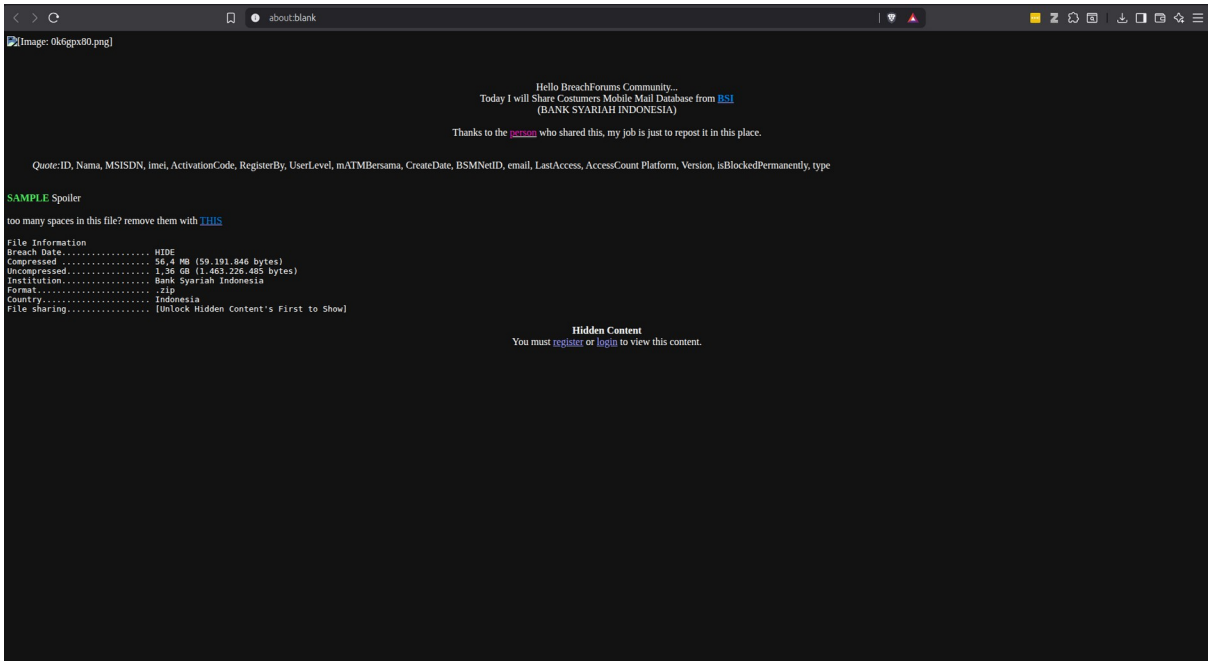


https://map.dataverso.net/whois

3.17. Os resultados das pesquisas no Console de CTI devem, no mínimo:
3.17.1. Retornar os seguintes campos: contexto pesquisado, data da menção e/ou exposição, data e hora de criação do alerta, idioma, endereço (web/deep web/dark web) e conteúdo original completo;

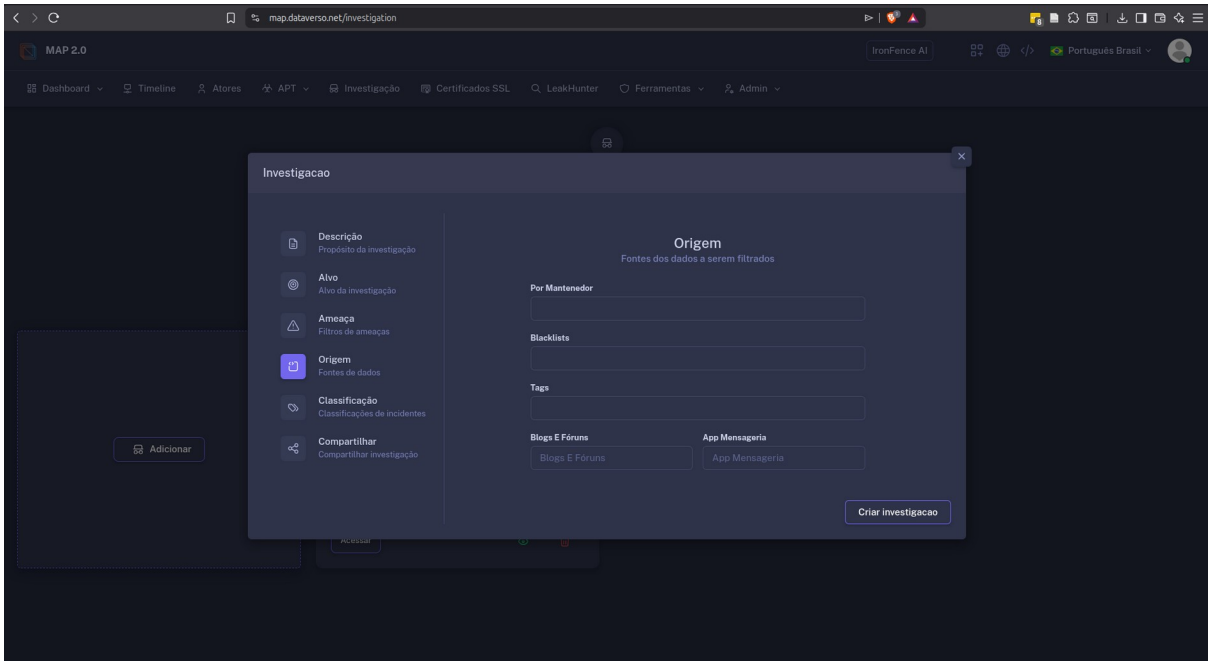


https://map.dataverso.net/feed



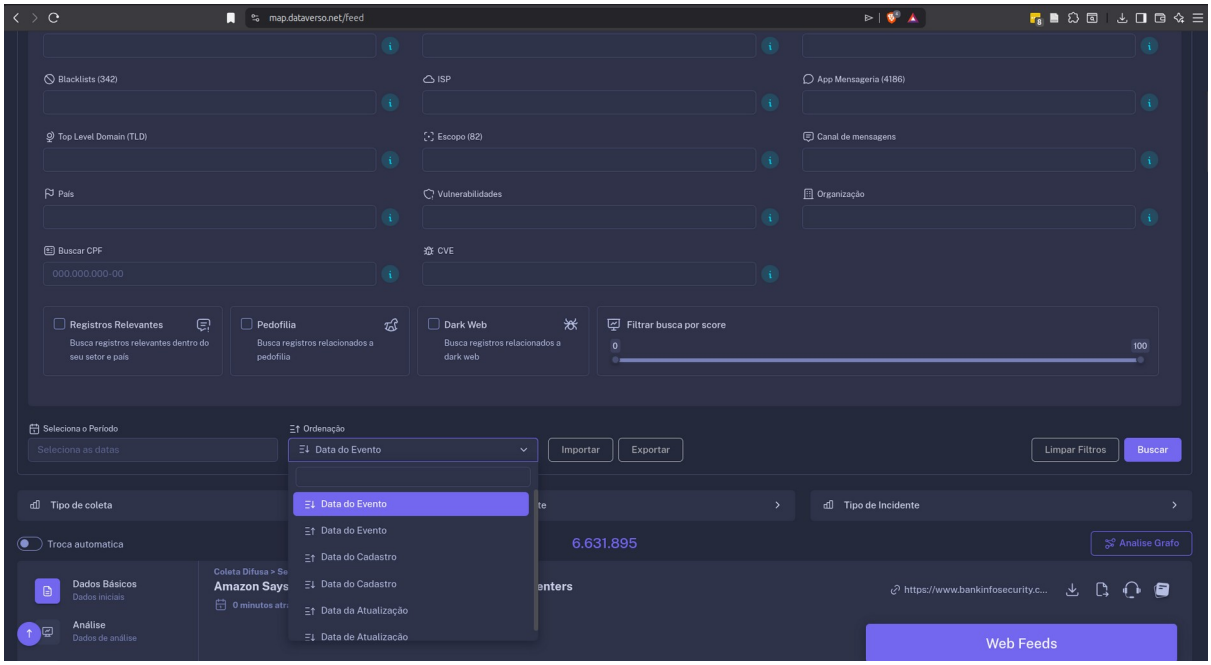
Clique em Fragmento de HTML

3.17.2. Permitir que as pesquisas sejam salvas para posterior verificação.



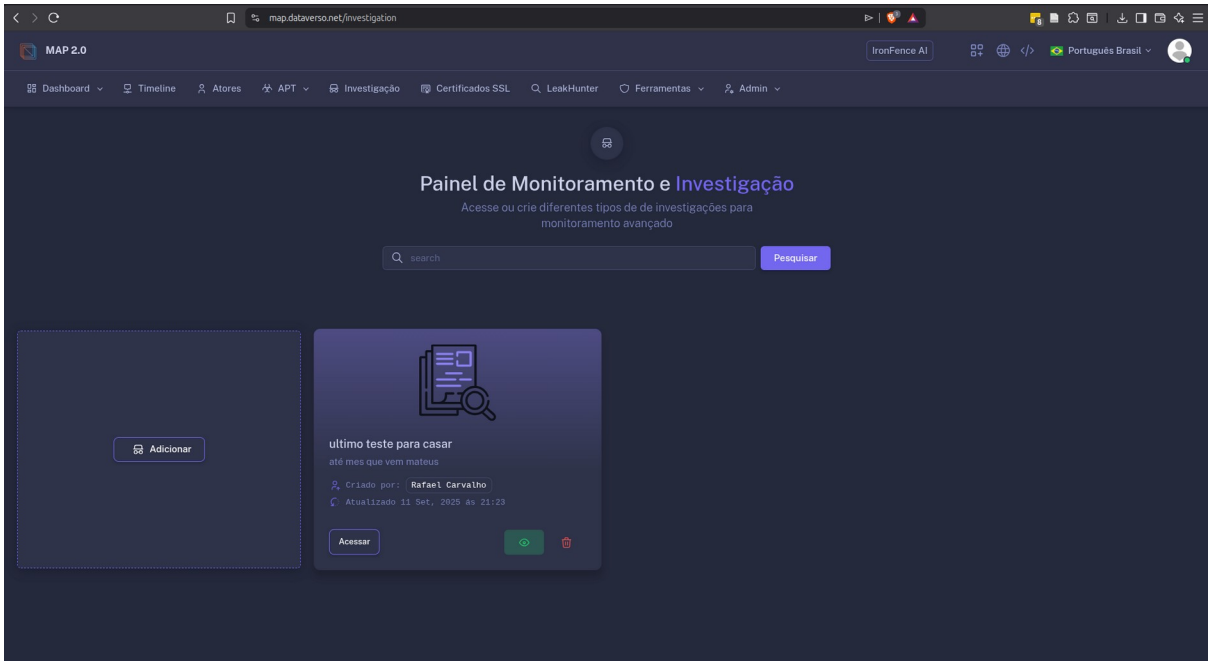
https://map.dataverso.net/investigation

3.17.3. Permitir que os resultados exibidos sejam ordenados conforme o interesse do usuário sendo ordenáveis por data e hora da ocorrência mais recente para a mais antiga, e por tema, ameaça, entre outros;



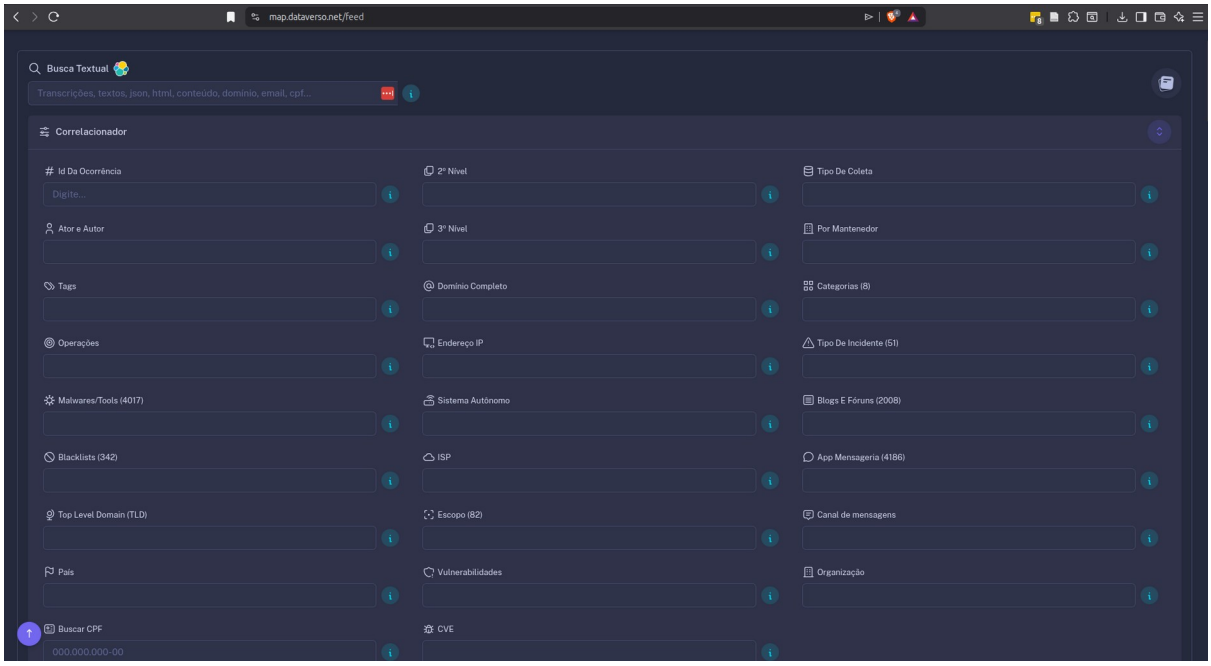
https://map.dataverso.net/feed

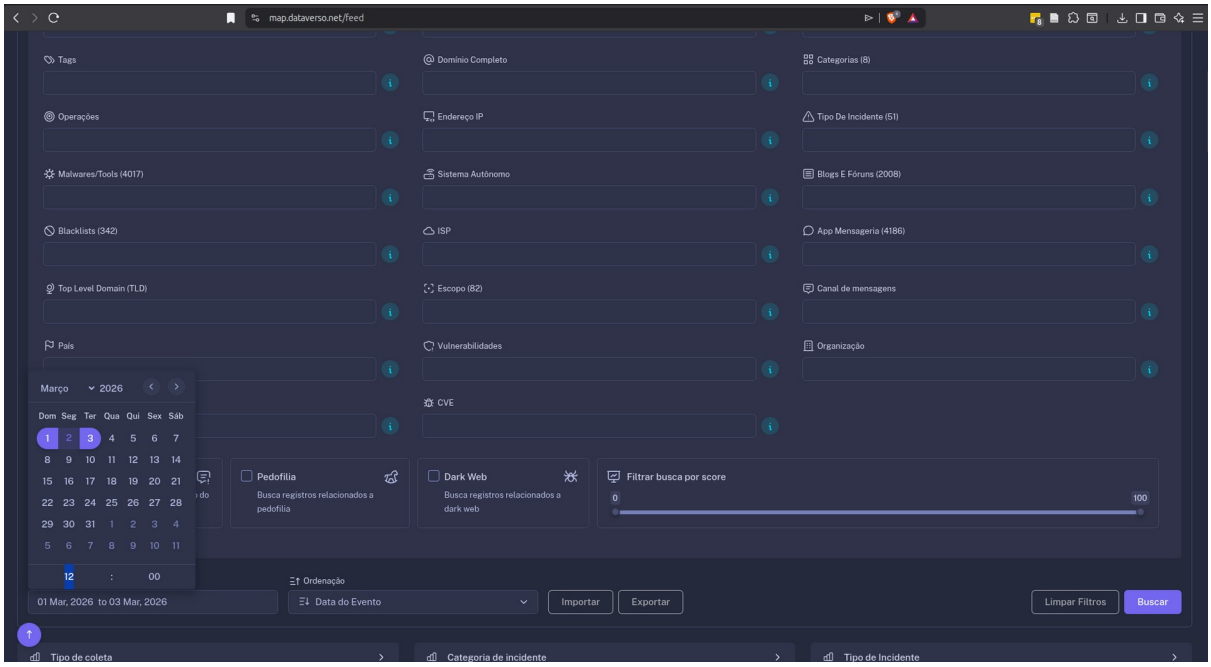
3.17.4. Permitir a atualização automática do resultado de pesquisas anteriormente realizadas com alertas visuais dessas atualizações;



Atualização no card de cada pesquisa construída
https://map.dataverso.net/investigation

3.17.5. Disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, contexto, metadados e tipo da fonte;

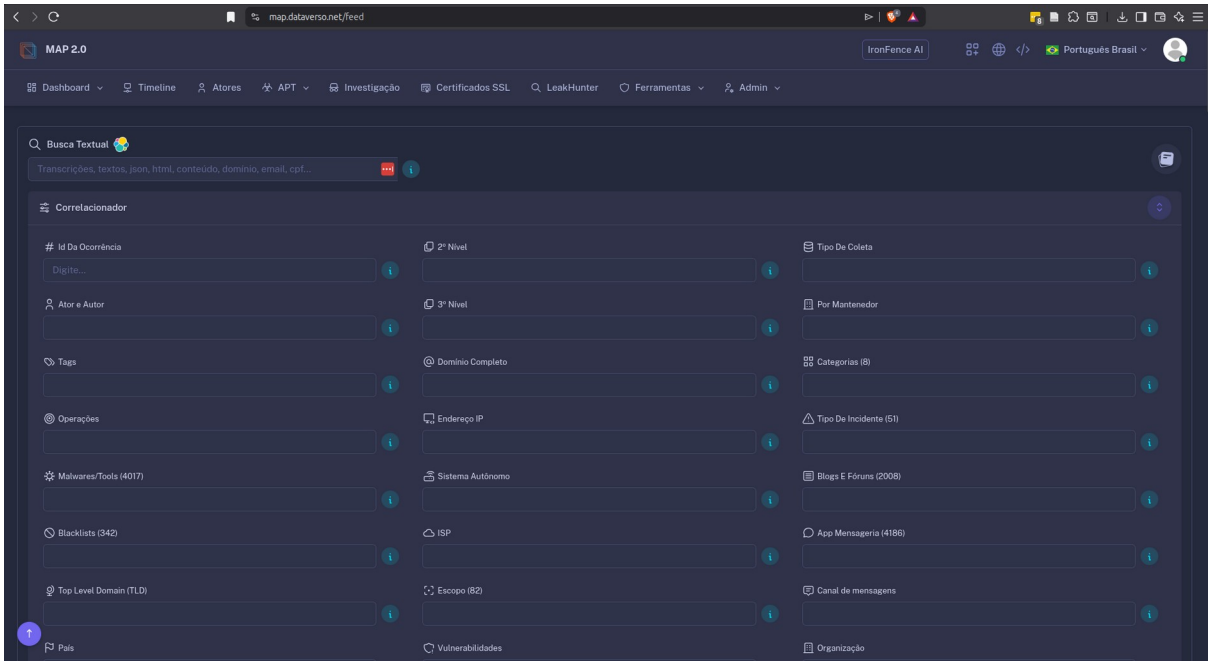




https://map.dataverso.net/feed

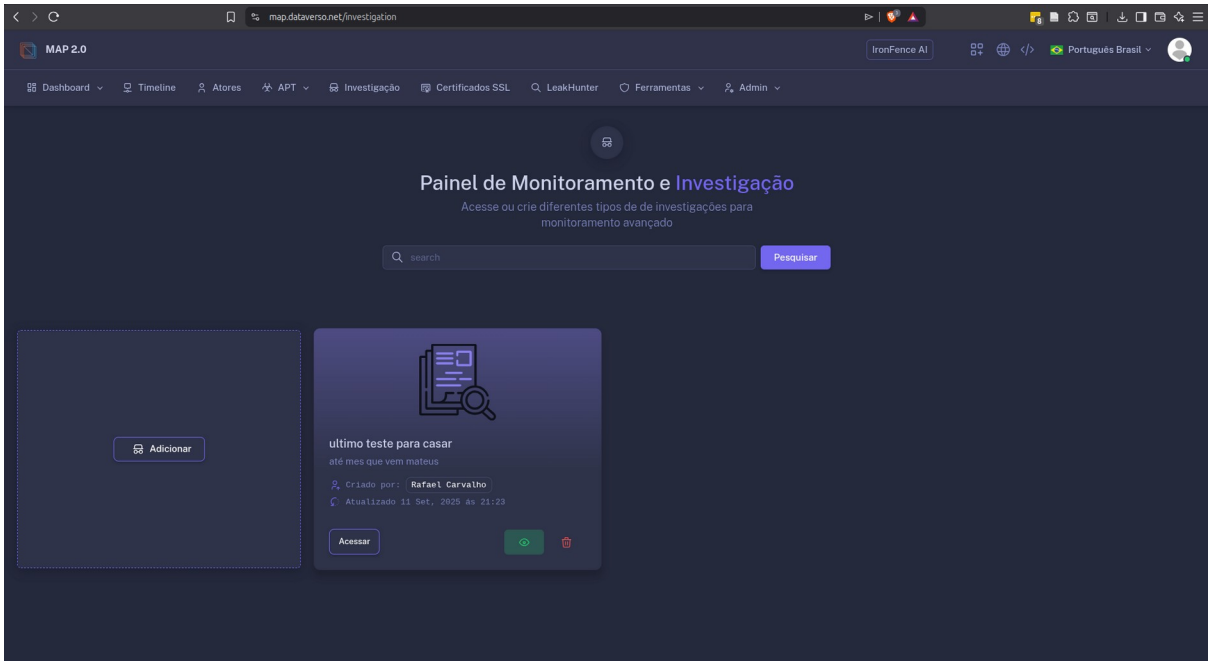
3.17.6. Possuir interface de fácil visualização para demonstrar os resultados das buscas por cada categoria de fonte realizada, (fontes abertas, fóruns, blogs, redes sociais, aplicativos de

mensagens instantâneas, deep web e dark web);



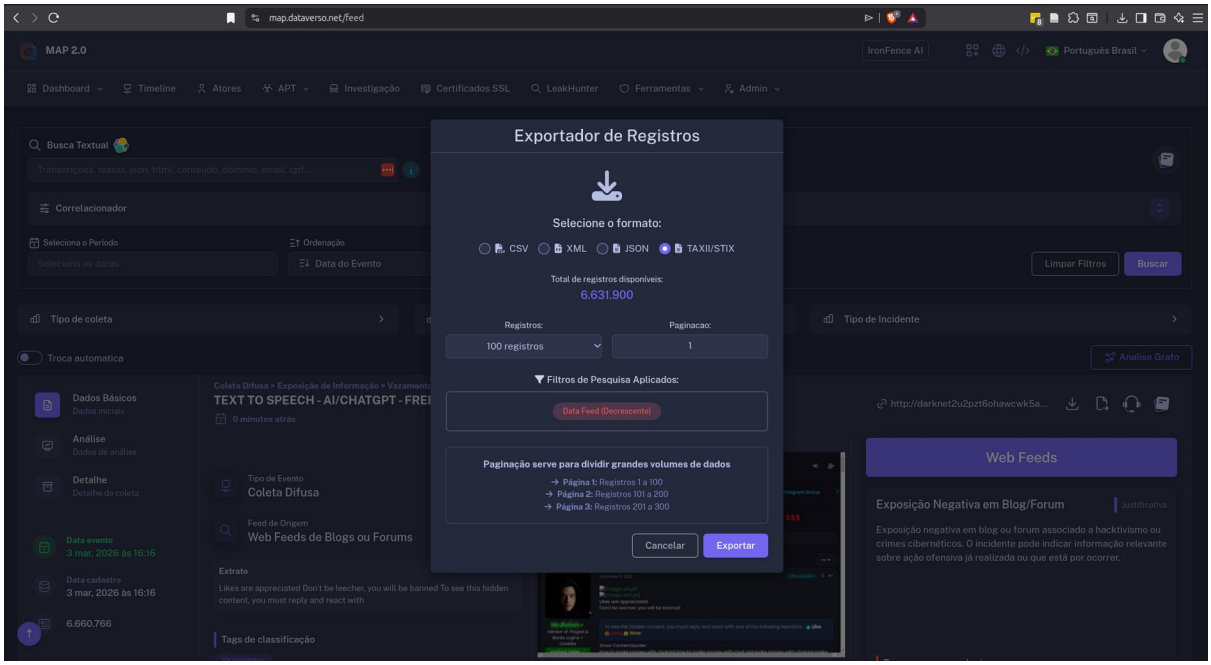
https://map.dataverso.net/feed

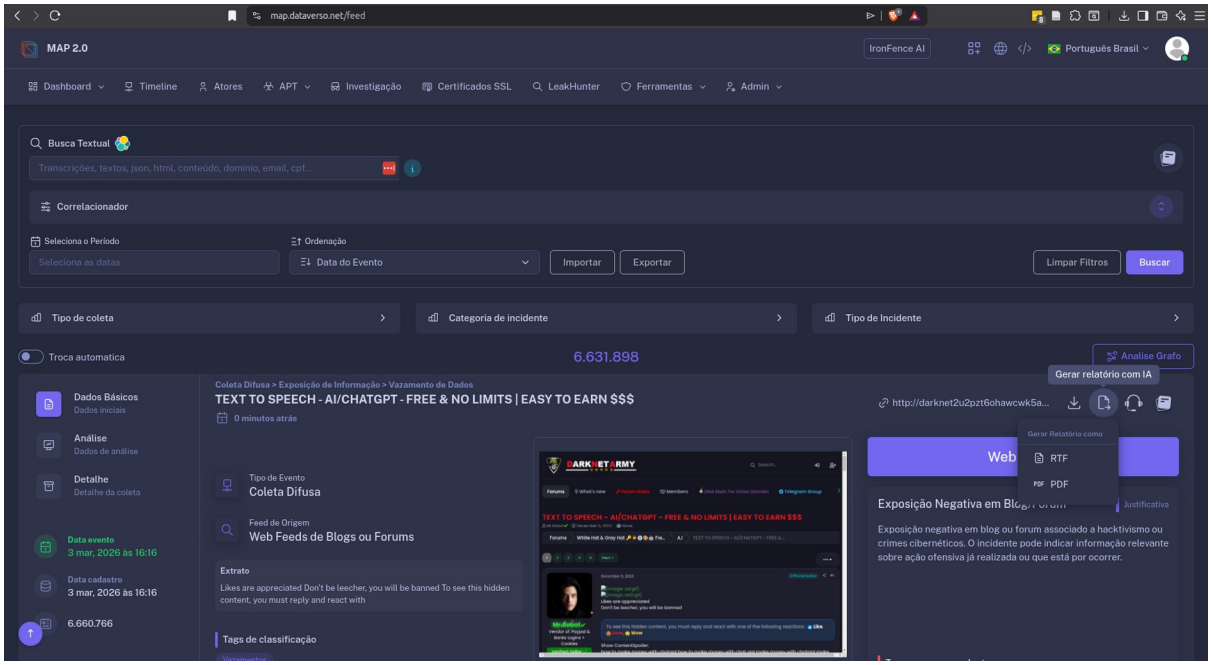
3.17.7. Disponibilizar uma tela com informações consolidadas para visualização das pesquisas realizadas e alertas cadastrados;



Atualização no card de cada pesquisa construída
https://map.dataverso.net/investigation

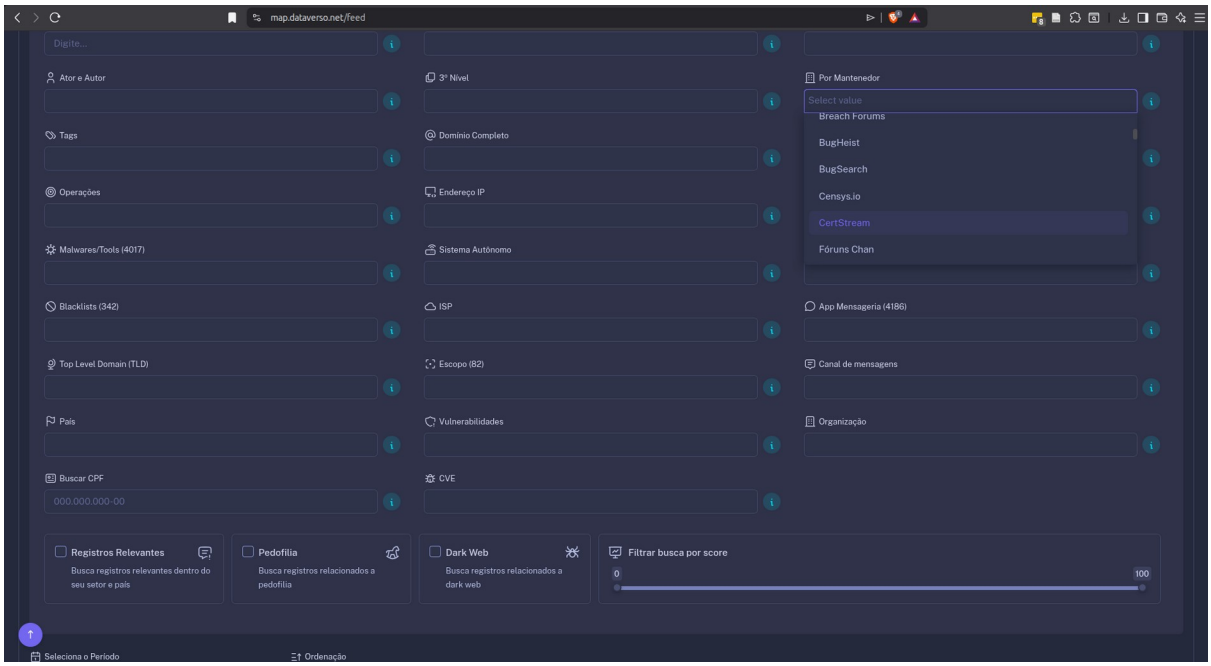
3.17.8. Permitir exportar qualquer pesquisa realizada de forma manual ou automática para os seguintes formatos: HTML, PDF, CSV, Planilha eletrônica e DOCX;





https://map.dataverso.net/feed - botão exportar

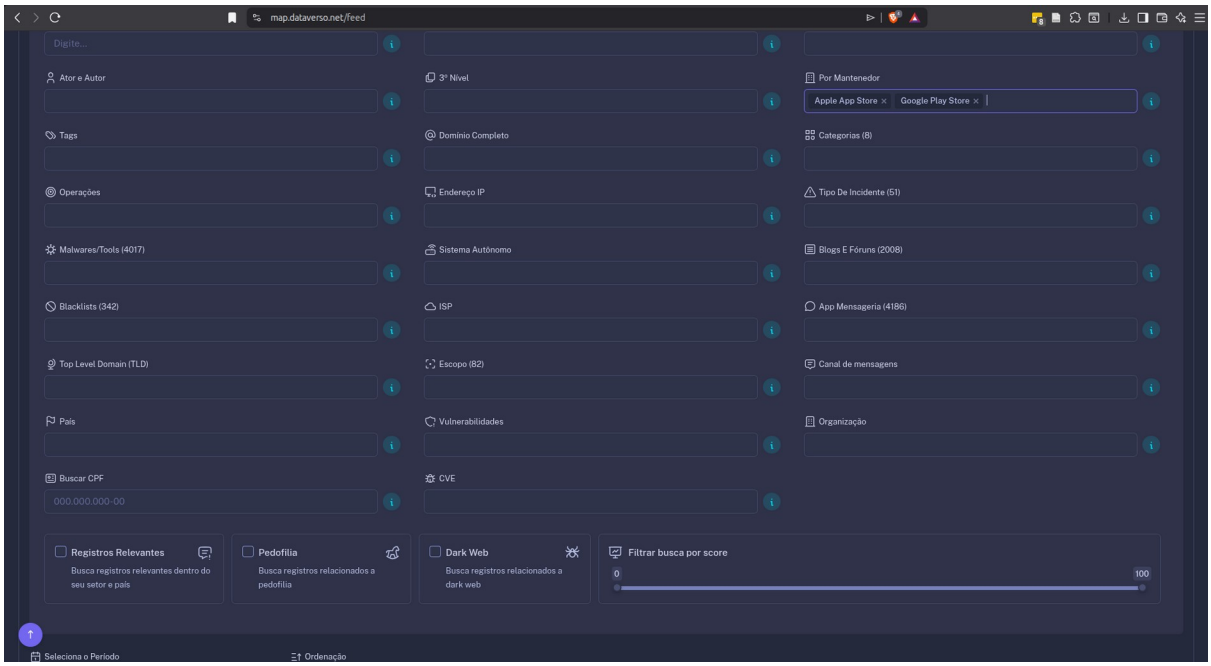
3.18. Este Serviço de INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS deve:
3.18.1. Monitorar ameaças contidas na internet aberta, deep web e dark web, em temas que possam ameaçar pessoas de interesse, ativos de informação e sistemas de TIC do BNB, do ponto de vista da segurança cibernética. O monitoramento nestes 3 ambientes compreende, mas não se limita, às mídias como: domínios, sites, blogs, vlogs, fóruns, chats de mensagens e redes sociais;



Lista “Por Mantenedor”

https://map.dataverso.net/feed

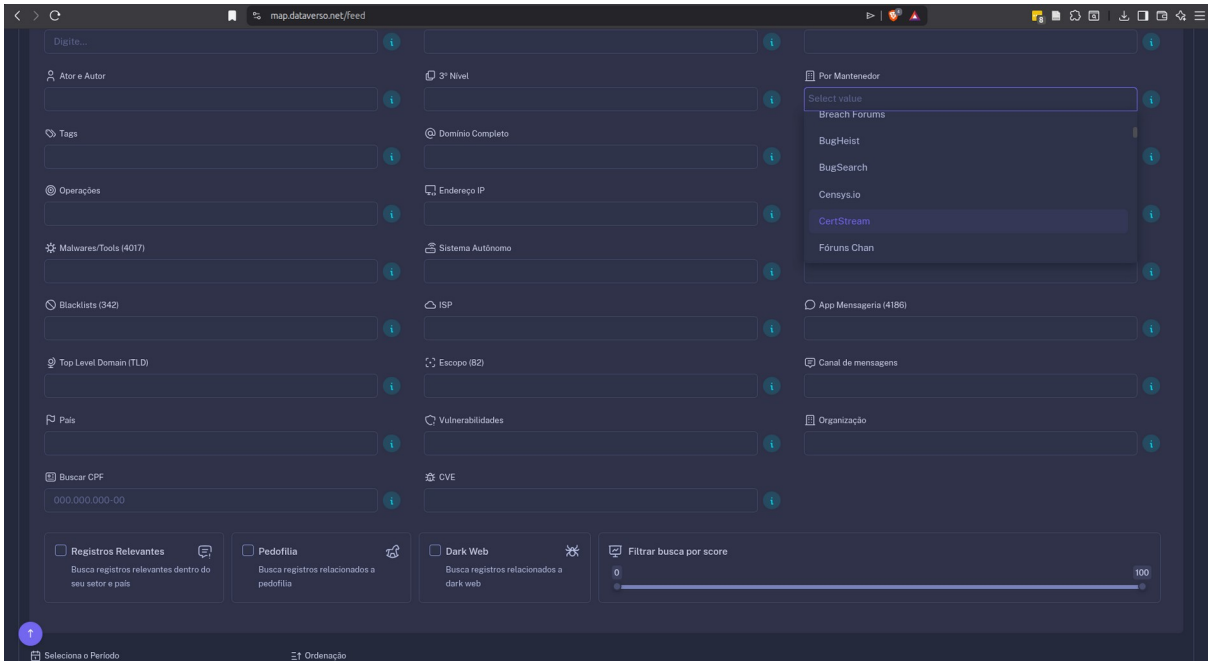
3.18.2. Monitorar as lojas de aplicativos Apple Store e Google Play com o objetivo de detectar aplicativos maliciosos que estejam relacionados com o BNB. É de responsabilidade da CONTRATADA providenciar a remoção de aplicações falsas e maliciosas através de parcerias com as lojas de aplicativos, quando solicitado pelo BNB;



Lista “Por Mantenedor”

https://map.dataverso.net/feed

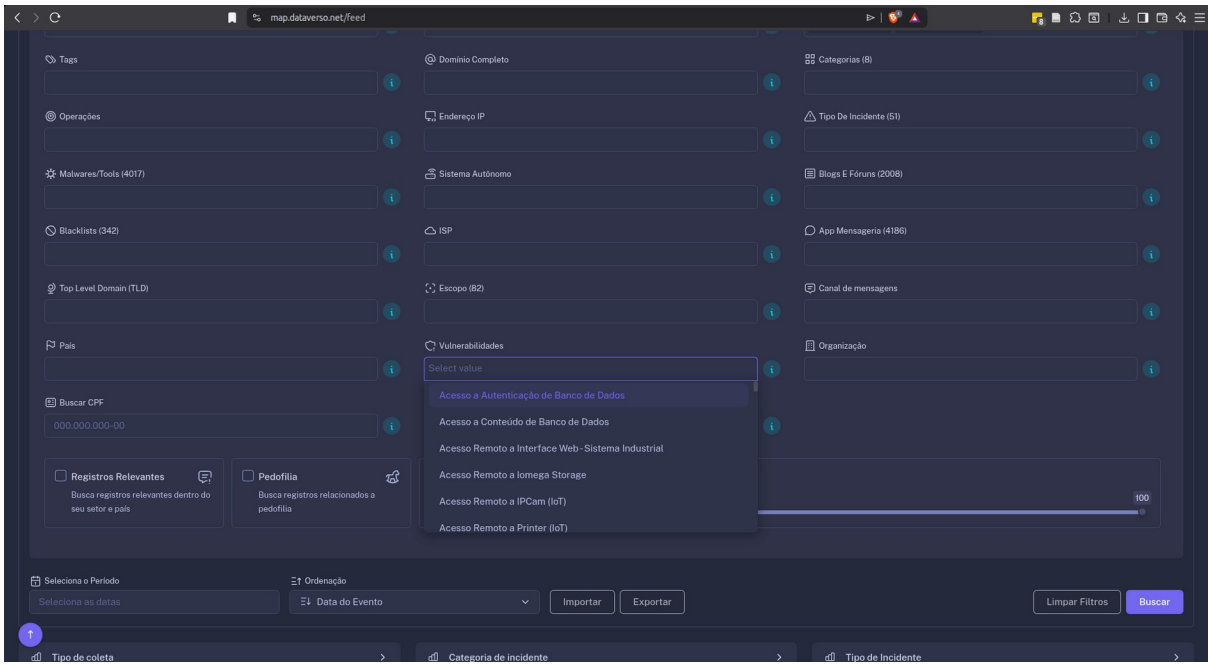
3.18.3. Monitorar fontes de informações como Shodan, BinaryEdge, Zone-H, Bases de CVE, entre outras, bem como sites que compartilhem informações sobre TTPs utilizados para ataques como phishing, ransomware, entre outros;



Lista “Por Mantenedor”

https://map.dataverso.net/feed

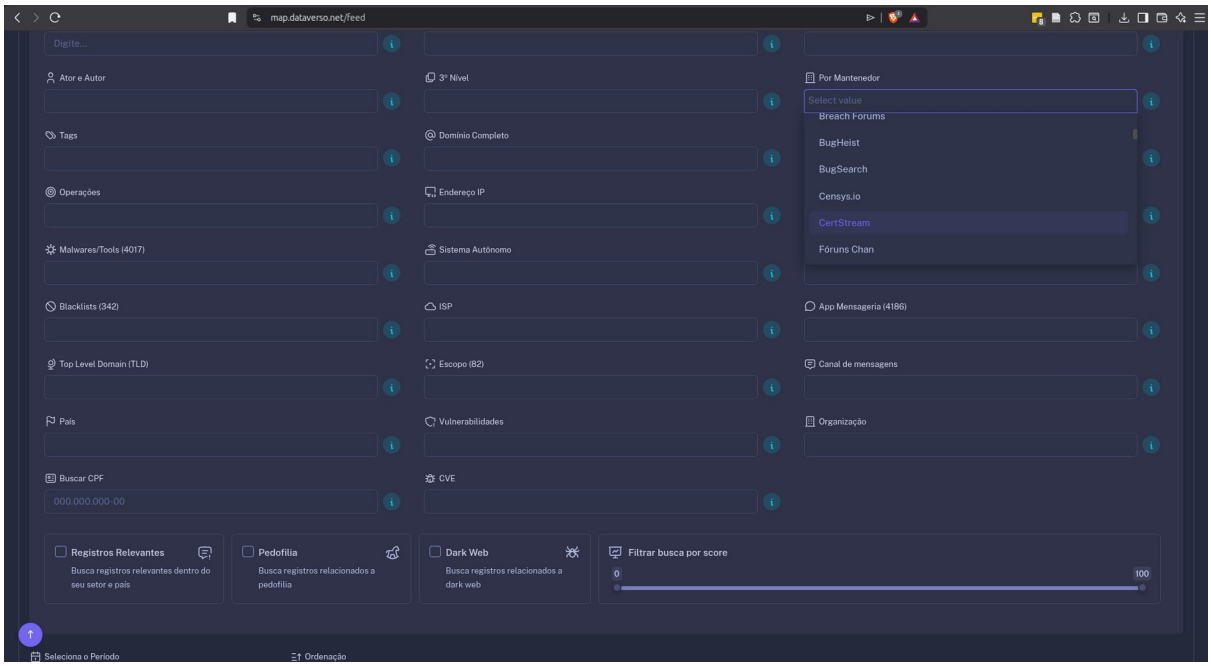
3.18.4. Monitorar listagem detalhada de serviços vulneráveis (DNS, NTP, FTP, SMB, etc.), vulnerabilidades clássicas (HeartBleed, Poodle, Logjam, etc.), Google Dorks para descoberta, registro com CVE, CWE, payload, geolocalização, provedor, protocolo, severidade (CVSS);



Lista “Vulnerabilidades”

https://map.dataverso.net/feed

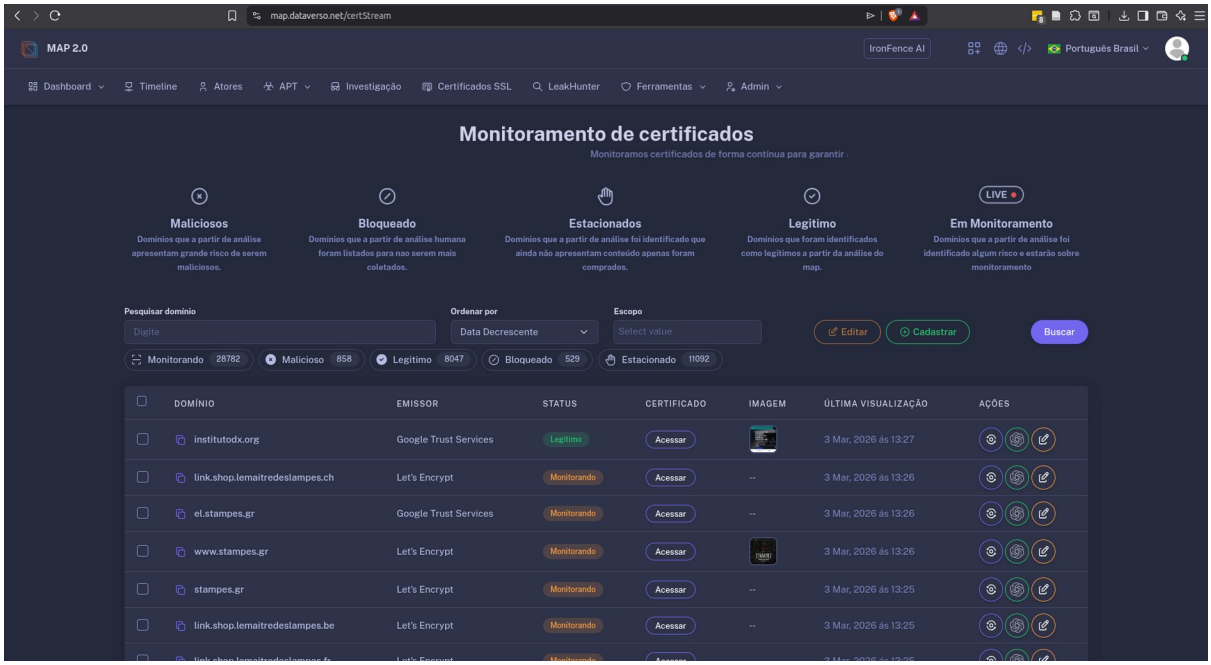
3.18.5. Monitorar ameaças cibernéticas contidas nas redes sociais em temas que possam ameaçar pessoas de interesse, ativos de informação e sistemas de TIC do BNB, do ponto de vista da segurança cibernética. As redes sociais, compreendem, mas não se limitam à: Twitter, Facebook, Youtube, Instagram, TikTok, LinkedIn, WhatsApp, Discord, Telegram, Pastebin, Ghostbin, Scribd, Reclame Aqui, Apple Store, 4Shared, Google Play, Vimeo e Github, Gitlab e feeds RSS;



Lista “Por Mantenedor”

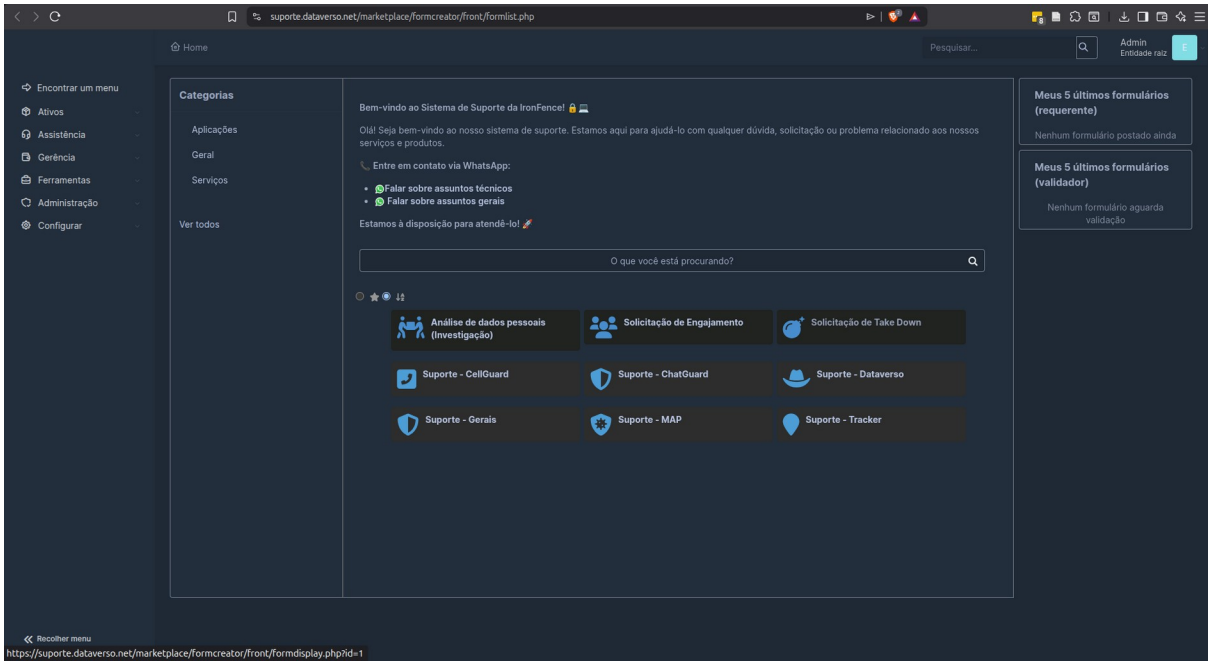
https://map.dataverso.net/feed

3.18.6. Monitorar ameaças representadas por domínios suspeitos ou fraudulentos e em seguida realizar o takedown desses domínios. A CONTRATADA se obriga a realizar todo o processo para retirada do ar desses sites que contenham phishing ou sites que disparem spam utilizando-se do nome, da marca ou da imagem do BNB, mesmo que similar, (com intuito de confundir e aplicar fraudes ou golpes nos usuários dos serviços prestados pelo BNB). A CONTRATADA deve prover serviço de monitoramento de domínios nacionais e internacionais, incluindo Top-Level Domain (TLDs) e Generic Top-Level Domain (gTLDs) e Country Code Top-Level Domain (ccTLD), que verifique a utilização do uso indevido das marcas do BNB no nome do domínio ou na URL, a empresa que administra o registro do domínio, e os dados do proprietário do domínio. A CONTRATADA deverá emitir um alerta, atualizado conforme andamento do atendimento, para acompanhamento do processo de takedown de cada ocorrência.



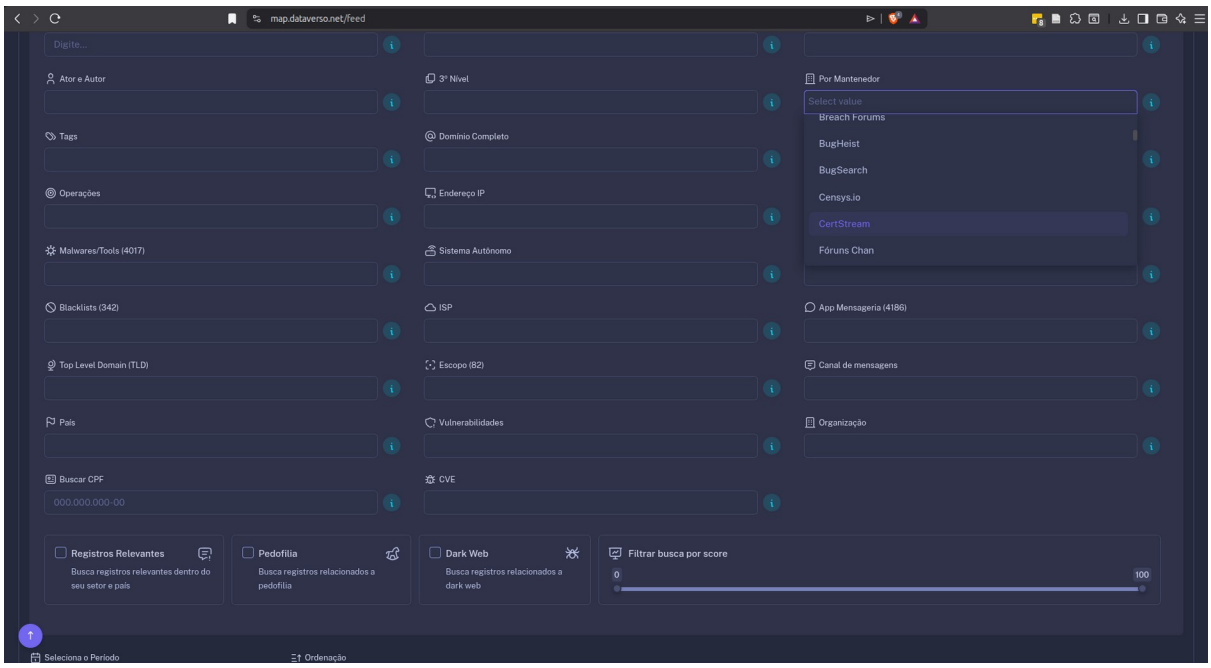
https://map.dataverso.net/certStream

3.18.7. Fruto do monitoramento do item anterior, pode ser necessário remover perfis falsos, desde que estejam relacionados com os ativos de informação monitorados. Será obrigação da CONTRATADA estabelecer parcerias com as principais redes sociais para os procedimentos de desativação desses perfis falsos, quando solicitado pelo BNB;



https://suporte.dataverso.net/marketplace/formcreator/front/formlist.php

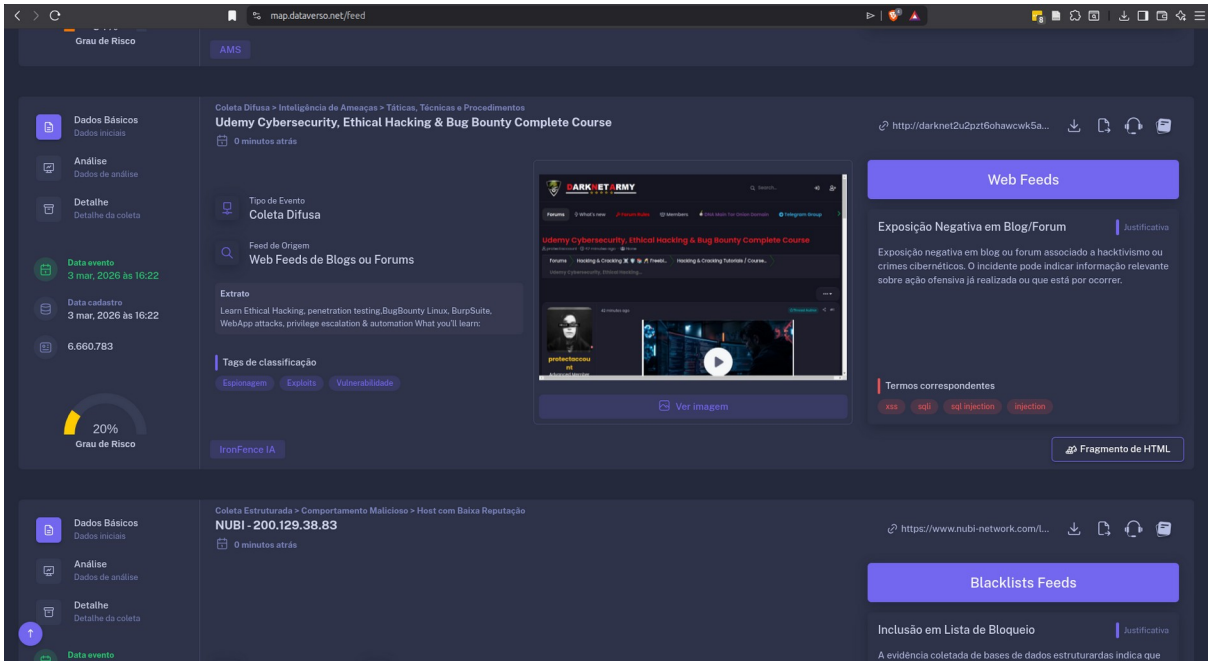
3.18.8. Monitorar ameaças, ataques e vulnerabilidades contidas em aplicativos de mensagens, como por exemplo WhatsApp e Telegram, em temas que possam ameaçar pessoas de interesse, ativos de informação e sistemas de TIC do BNB, do ponto de vista da segurança cibernética;



Lista “Por Mantenedor”

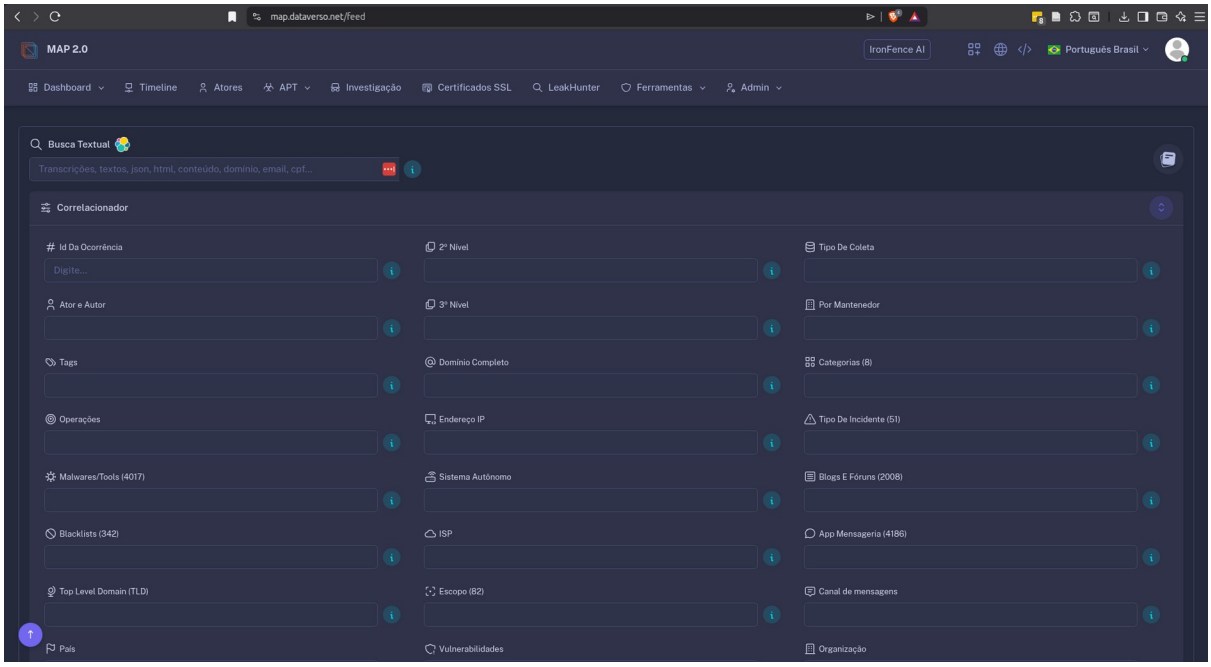
https://map.dataverso.net/feed

3.19. A solução deve fornecer um painel de visualização que contemple, no mínimo:
3.19.1. Visualização de eventos relacionados às palavras-chaves;



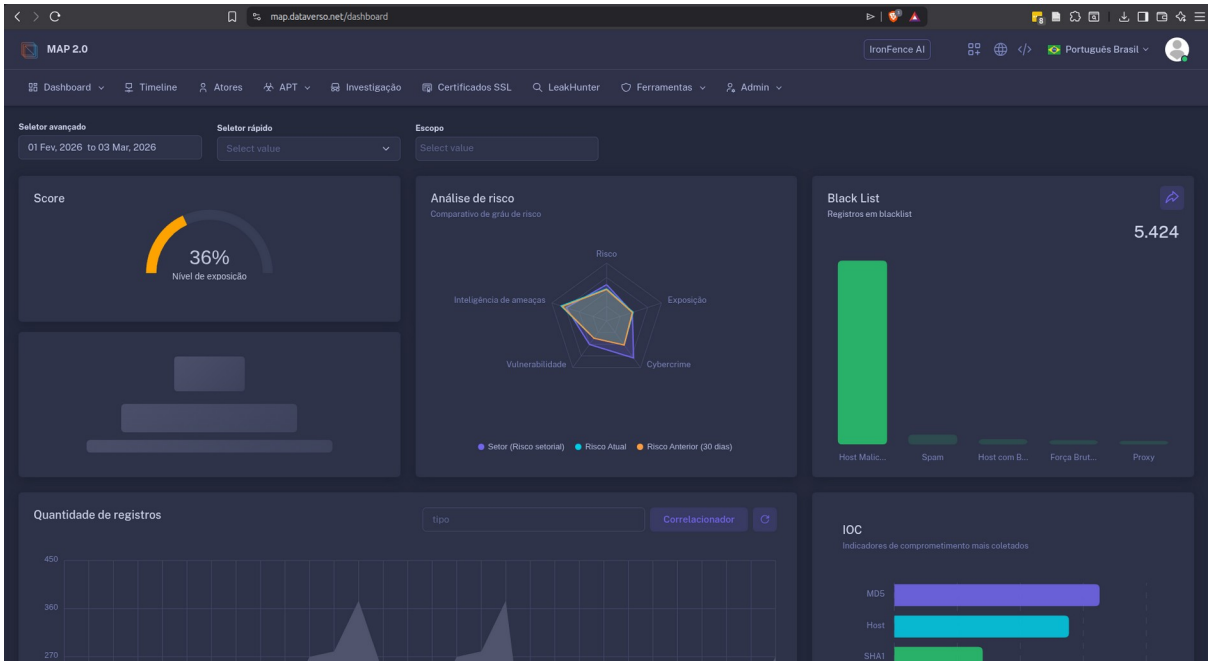
Termos correspondentes

3.19.2. Realização de buscas nos dados incluindo buscas avançadas com critérios e entidades diferentes;



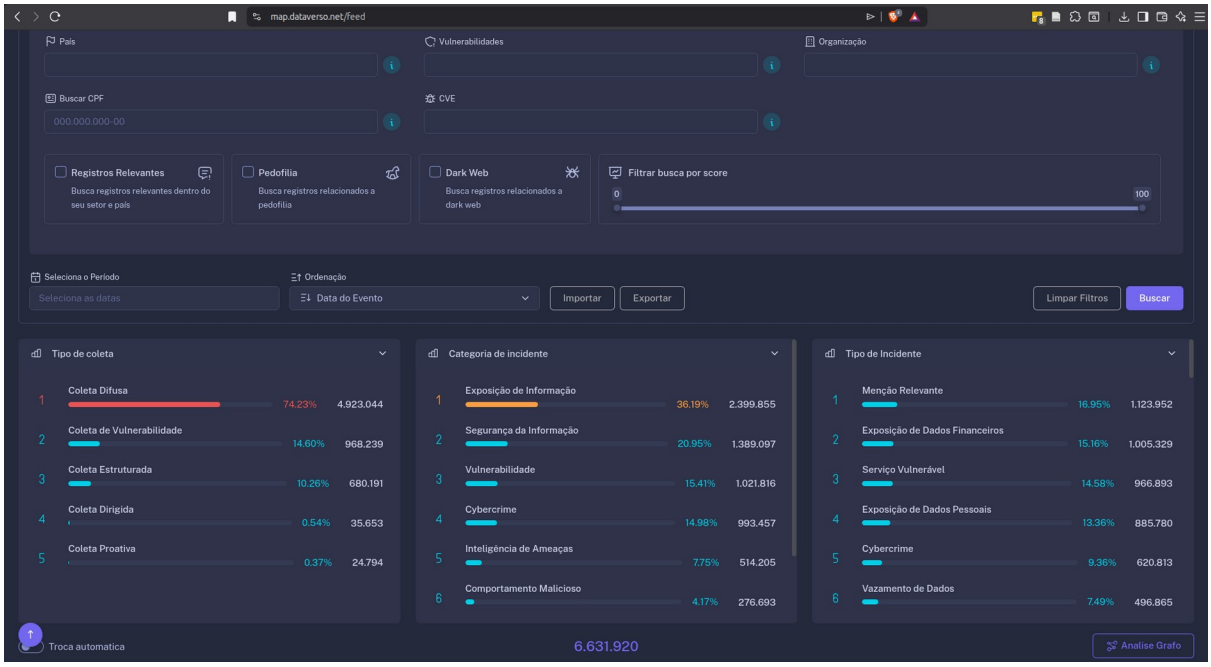
https://map.dataverso.net/feed

3.19.3. Navegação com clicks nos tipos de informações de interesse do painel, com apresentação das informações relacionadas.



https://map.dataverso.net/dashboard

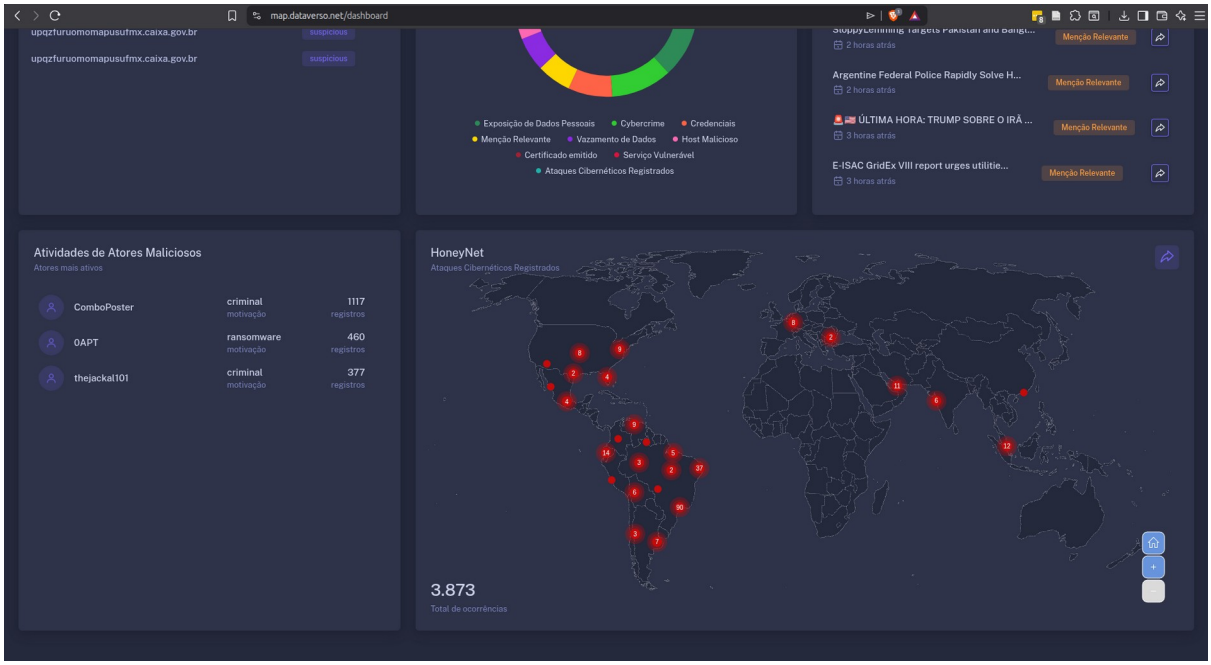
3.19.4. Apresentação dos dados buscados em painéis com as principais fontes identificadas na busca;



https://map.dataverso.net/feed

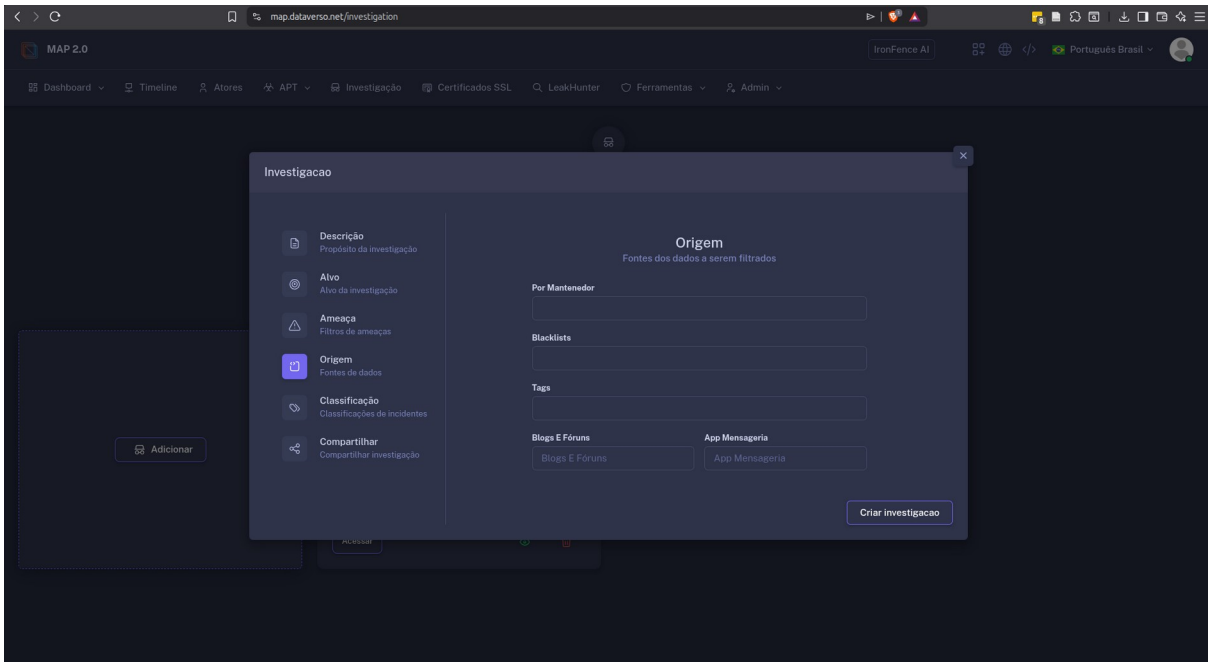
3.20. A solução deve possuir um dashboard para análise dos dados coletados com, no mínimo:

3.20.1. Gráfico com a quantidade de informações de acordo com palavras ou termos buscados;
3.20.2. Divisão dos dados por tipo de dado encontrado (imagem, texto, áudio etc.);
3.20.3. Principais perfis;
3.20.4. Principais fontes de dados;
3.20.5. Principais grupos.



https://map.dataverso.net/dashboard

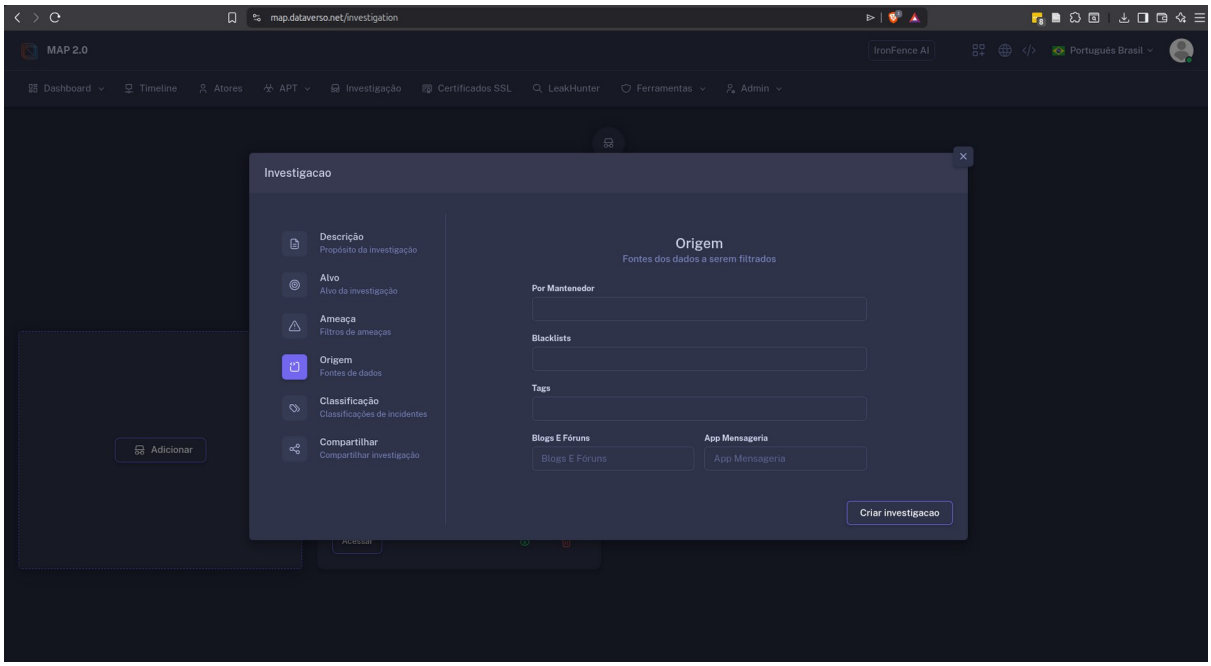
3.21. A solução deve permitir configuração de alertas diretamente via interface de gerenciamento.



https://map.dataverso.net/investigation

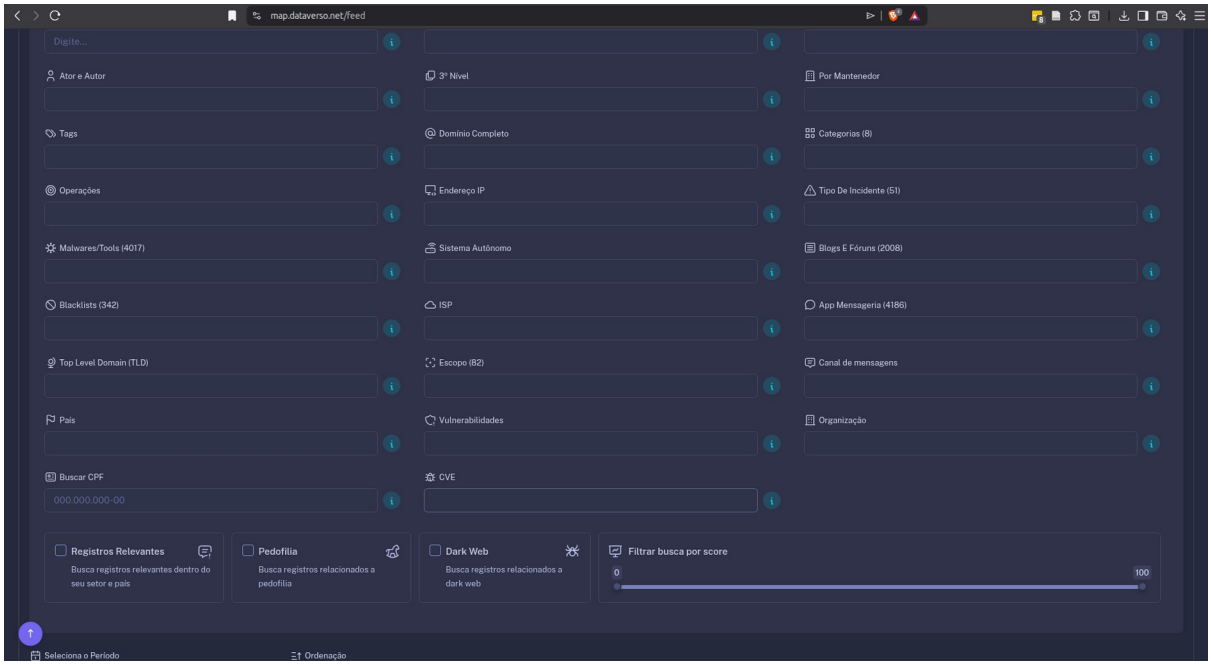
3.22. A solução deve permitir, através da interface de gerenciamento, que se realizem testes de

funcionamento dos alertas configurados, bem como também deve permitir a configuração de envio de alertas, no mínimo, via e-mail e SMS.

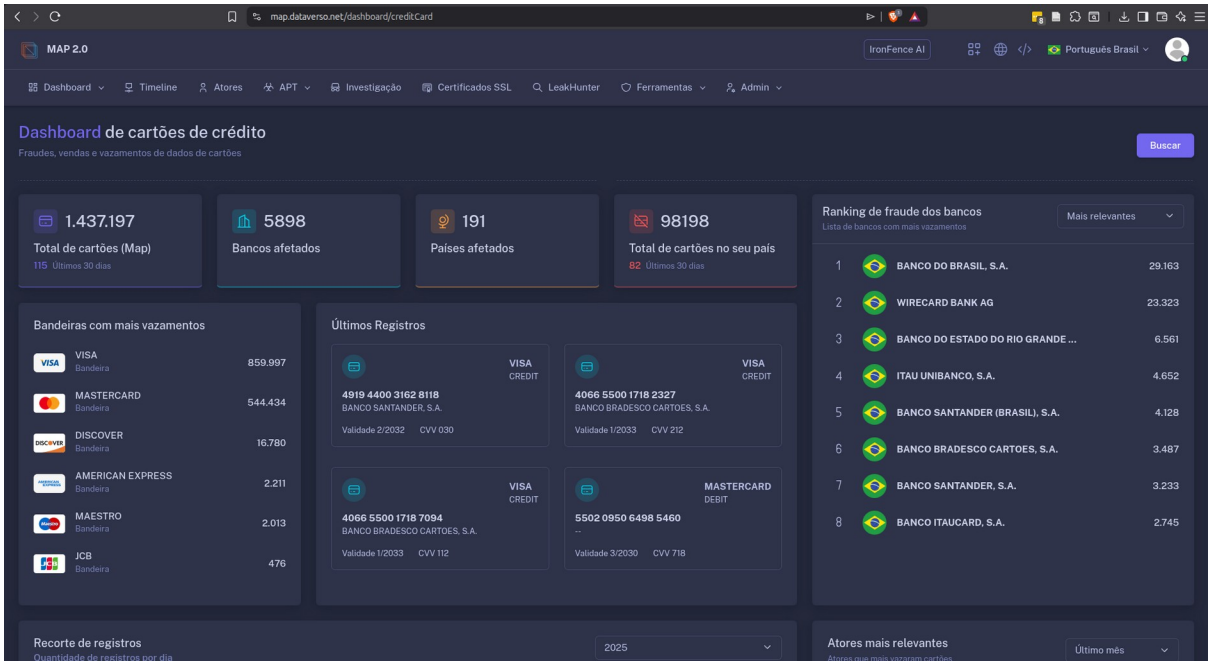


https://map.dataverso.net/investigation

3.23. A solução deve permitir a configuração de alertas baseados em:
3.23.1. consultas/pesquisas salvas;
3.23.2. CPF vazado/exposto;
3.23.3. citações de pessoas importantes (VIP);
3.23.4. credenciais de domínios cadastrados;
3.23.5. cartão de crédito vazados.

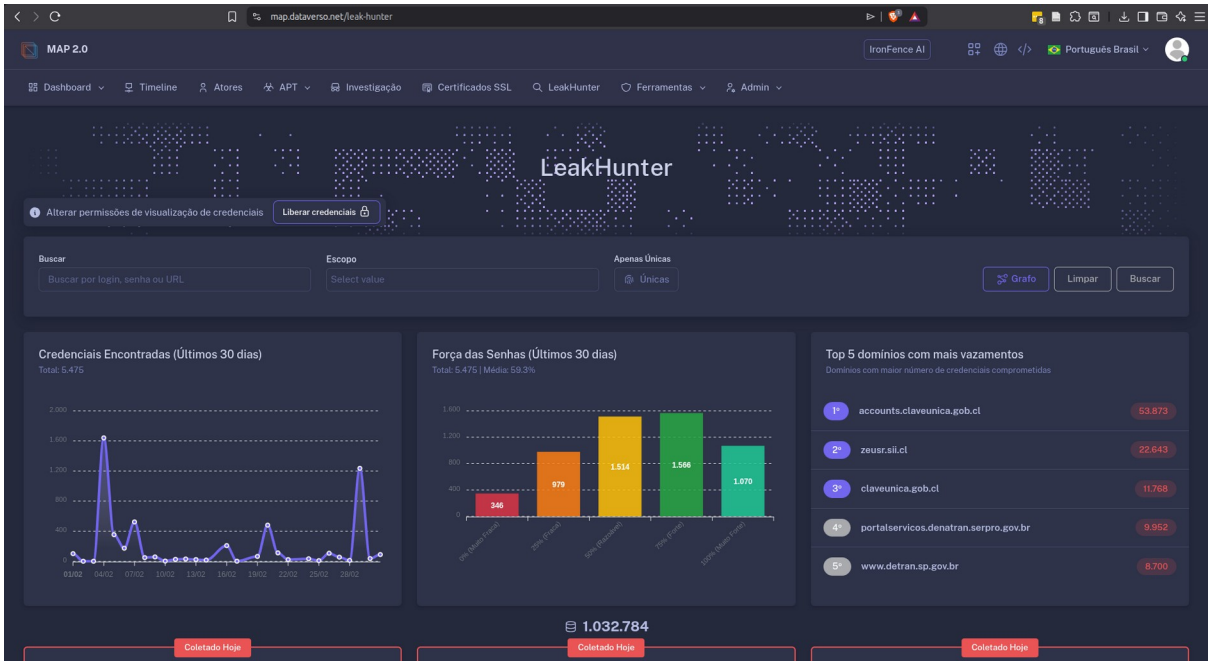


https://map.dataverso.net/feed



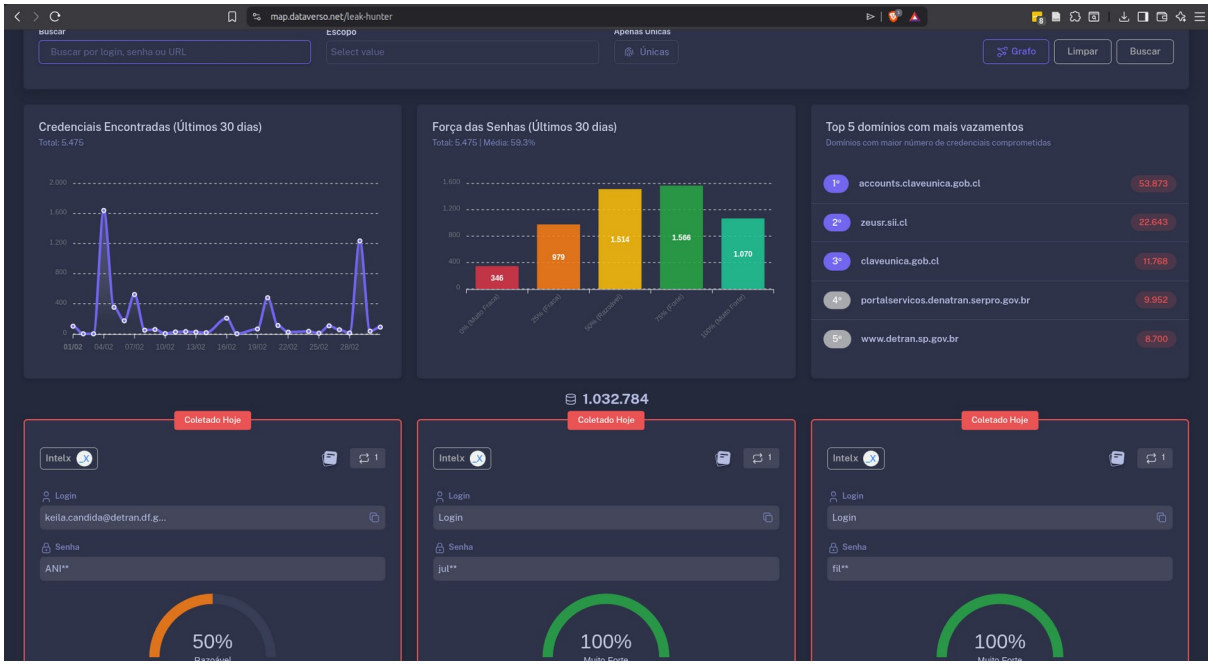
https://map.dataverso.net/dashboard/creditCard

3.24. A solução deve permitir filtrar os resultados da busca por data de recebimento da credencial vazada e por tipo de vazamento.



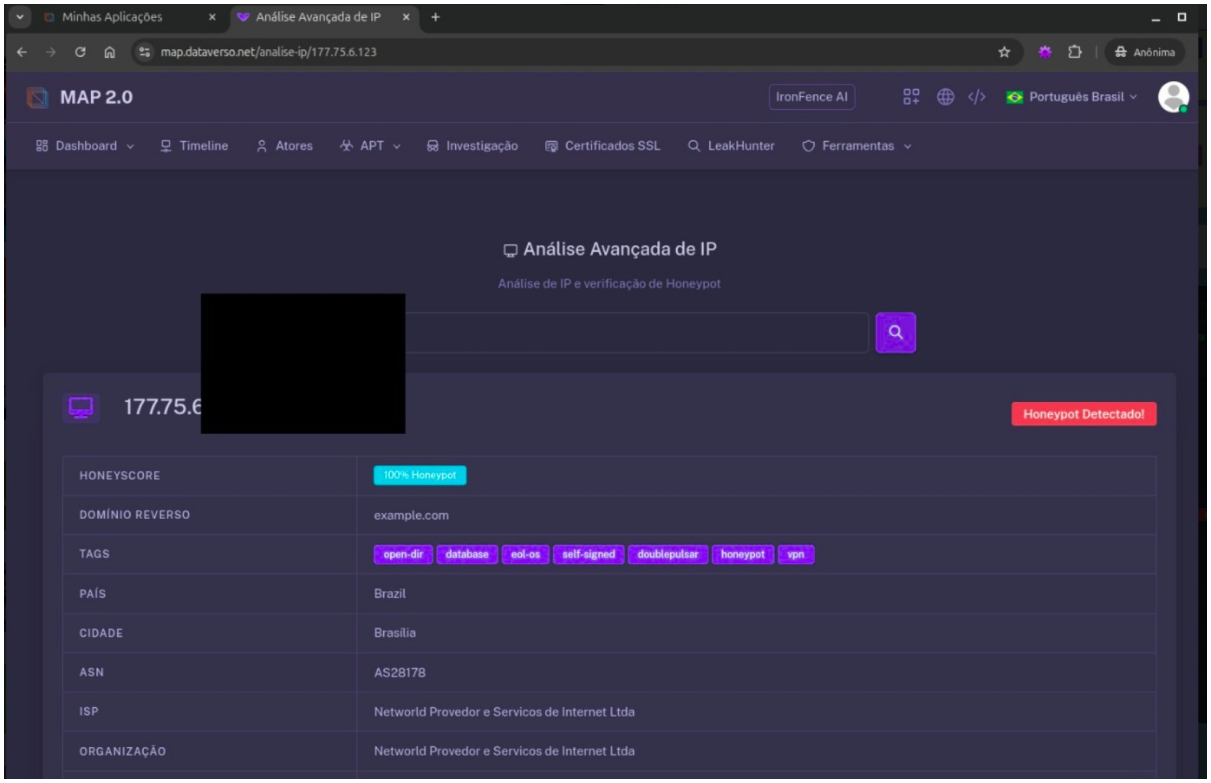
https://map.dataverso.net/leak-hunter

3.25. A solução deve permitir filtrar os resultados da busca por credenciais internas ou por credenciais de terceiros em domínios institucionais.

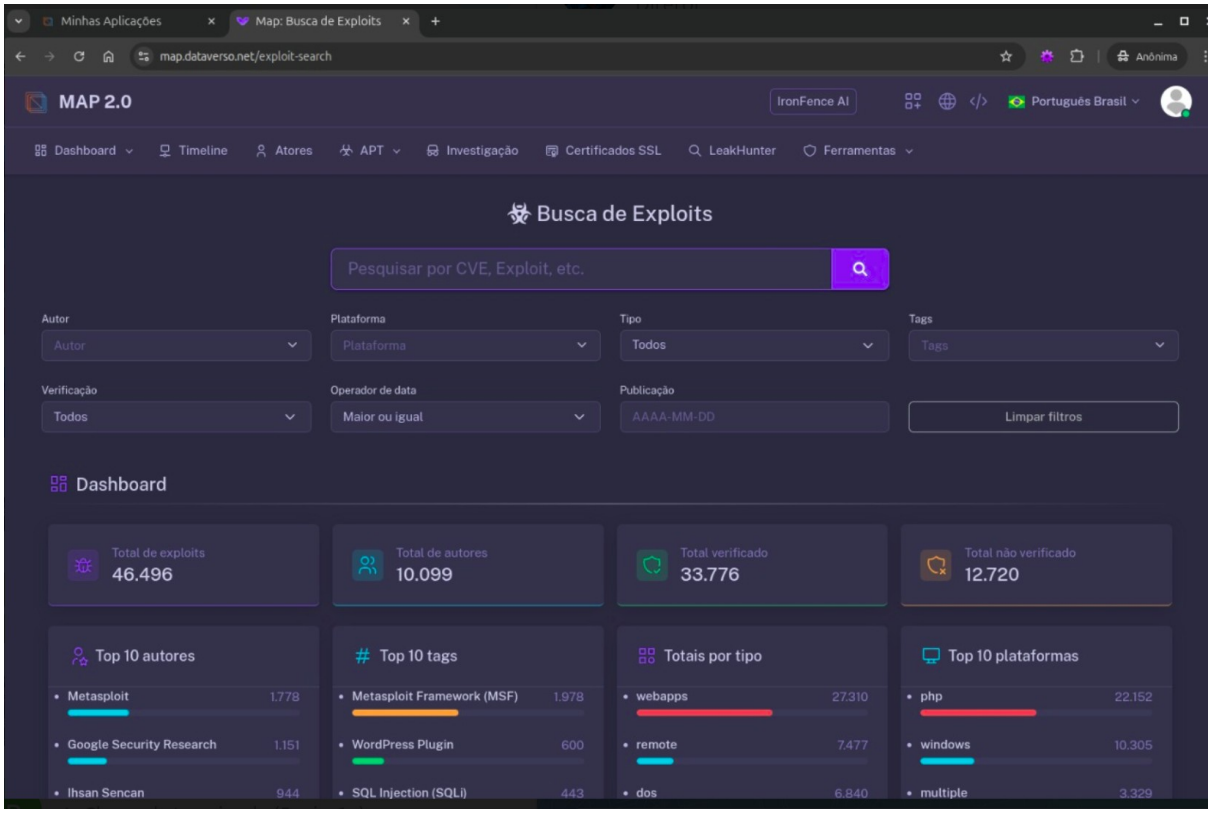


https://map.dataverso.net/leak-hunter
Buscar por credenciais específicas

3.26. A solução deve fornecer busca direta por IP com honeyscore, de exploits integrada à base (ExploitDB/Metasploit).

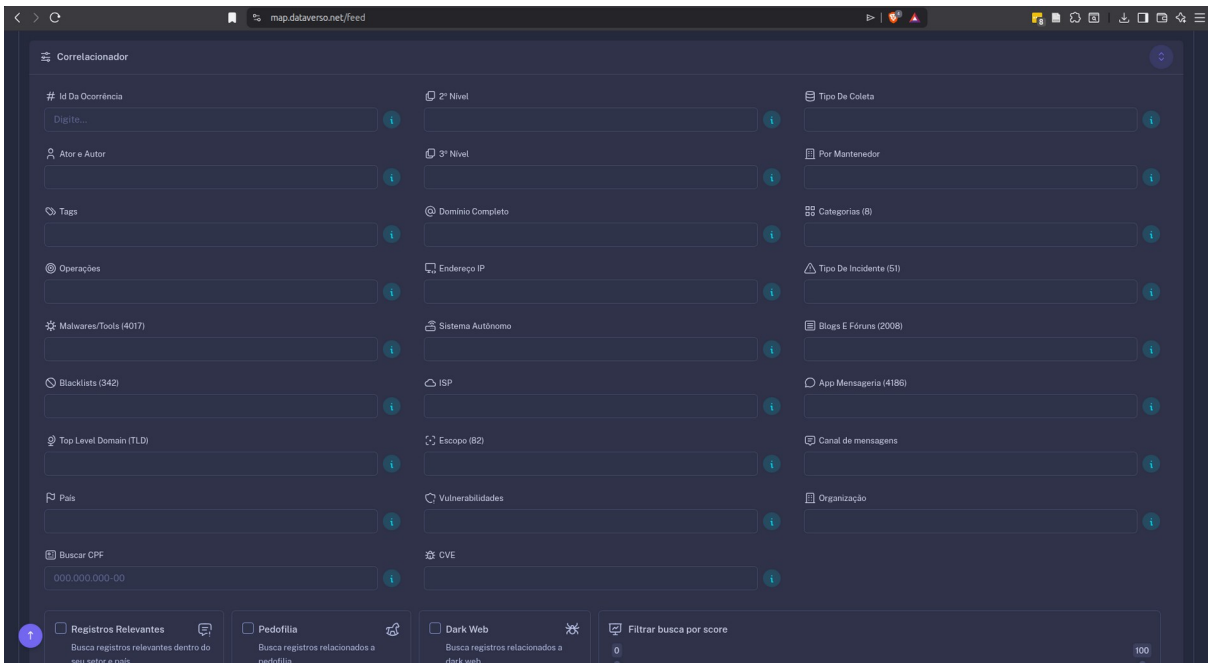


Análise de um IP com score de Honeypot, vulnerabilidades, portas abertas, CVEs e expolits, vinculados ao IP



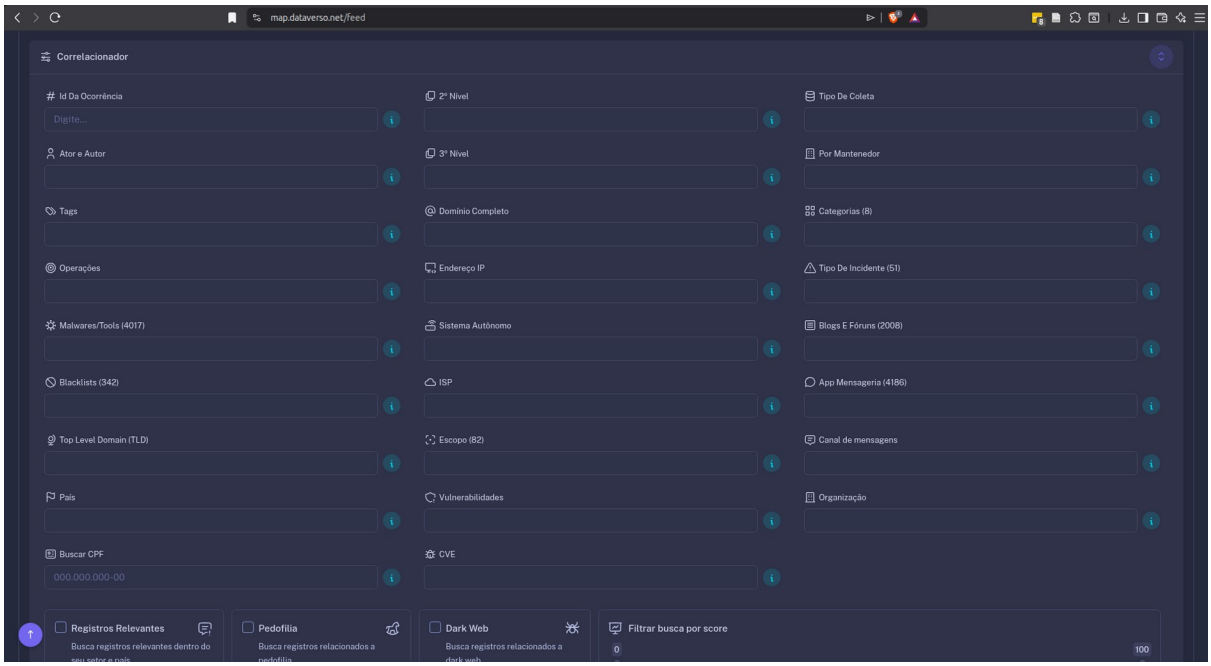
Base completa de Exploits e CVEs para consulta

3.27. A solução deve fornecer filtros personalizados que possibilitem a consulta de incidentes por campos diversos, tais como, URL, IP, data, status, assunto e remetente.



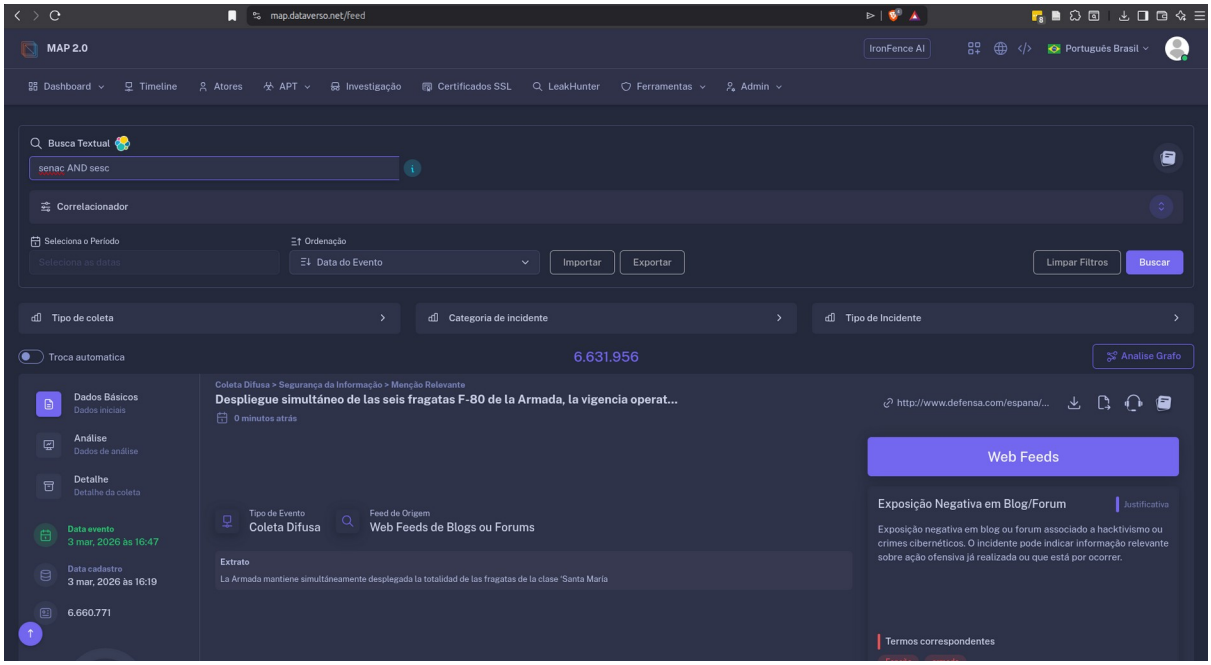
https://map.dataverso.net/feed

3.27.1. A solução deve disponibilizar mecanismo para busca das informações, permitindo buscas por intervalo de data, metadados específicos, fontes de informação, palavras-chaves, bem como por perfis específicos, usando nome/apelido, número de telefone ou e-mail, com no mínimo os seguintes campos: fonte; nome; apelido; telefone; e grupos.



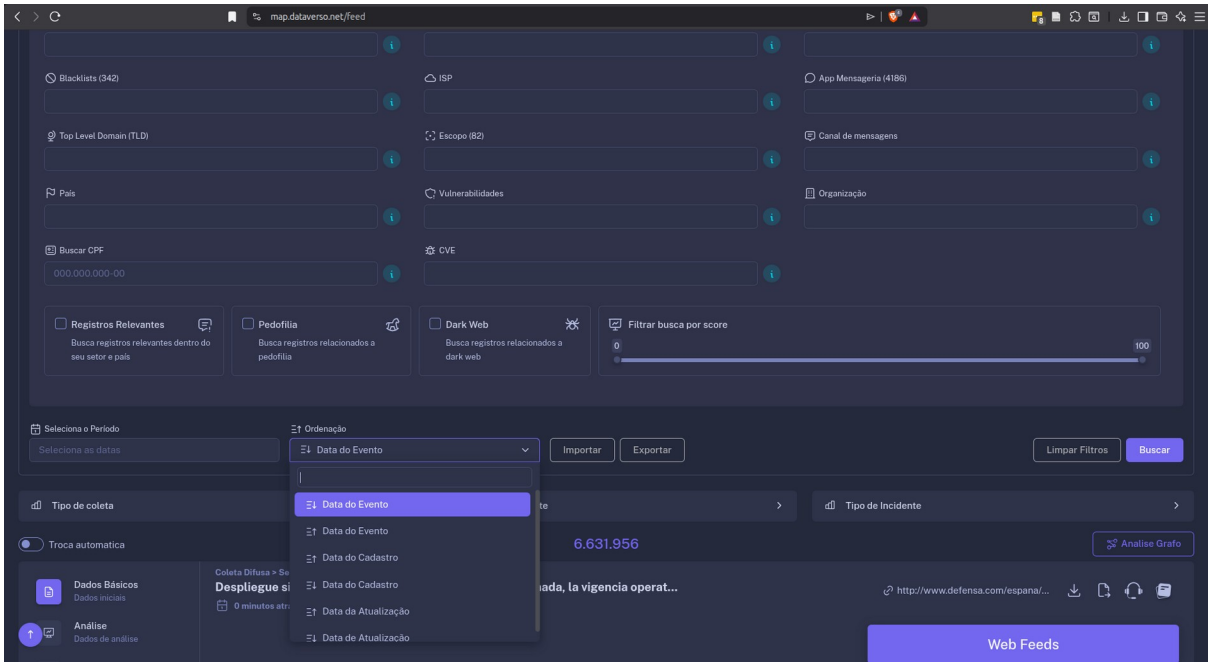
https://map.dataverso.net/feed

3.28. A solução deve disponibilizar, através de interface web, busca utilizando mecanismos como: proximidade, lógica fuzzy (difusa), lógica binária, expressões regulares (regex), operadores lógicos (“AND, “OR” e “NOT”) e caracteres wildcard (coringa).



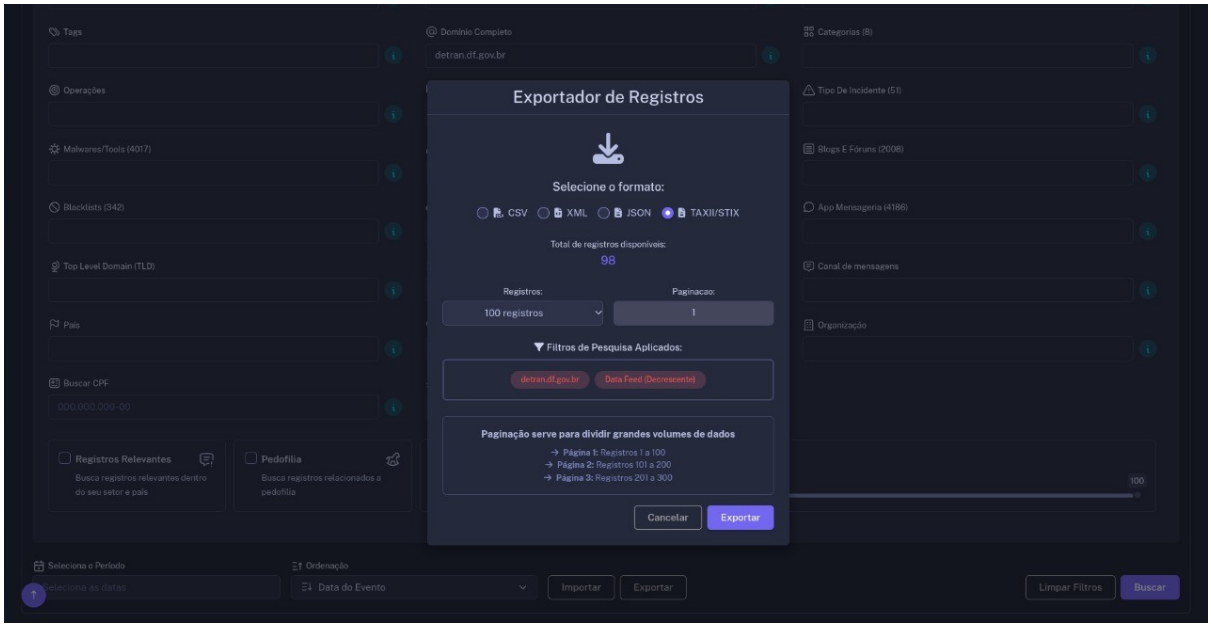
https://map.dataverso.net/feed

3.29. A solução deve permitir a ordenação dos resultados por data da postagem mais recente para a mais antiga.



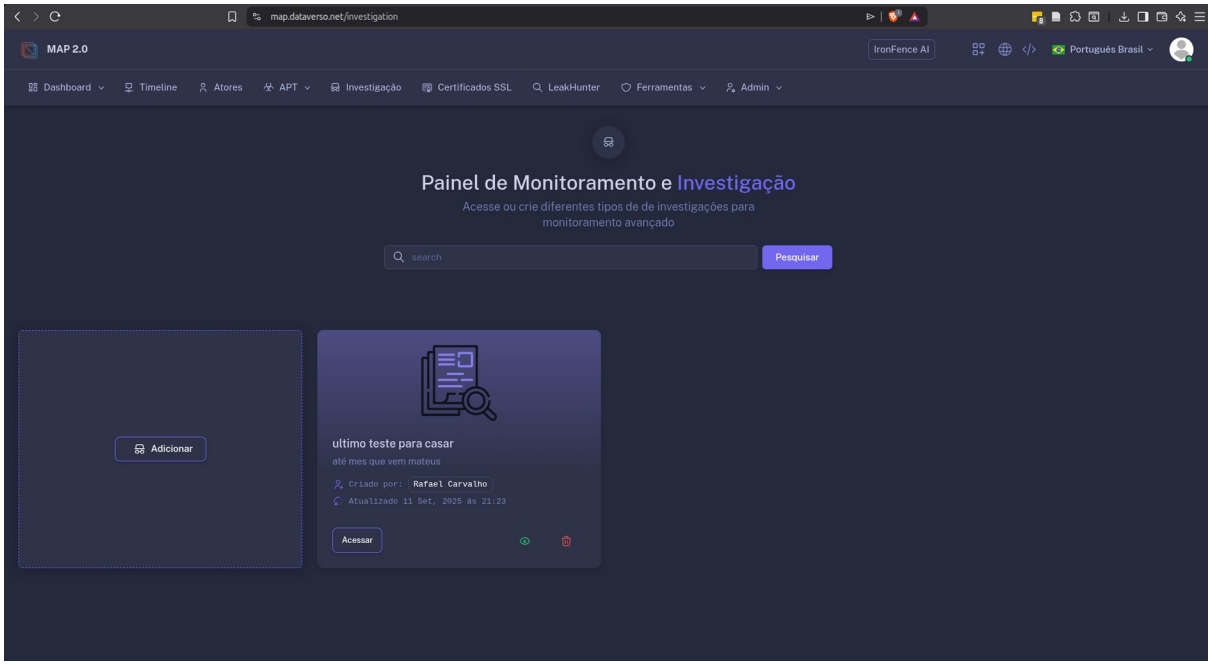
https://map.dataverso.net/feed

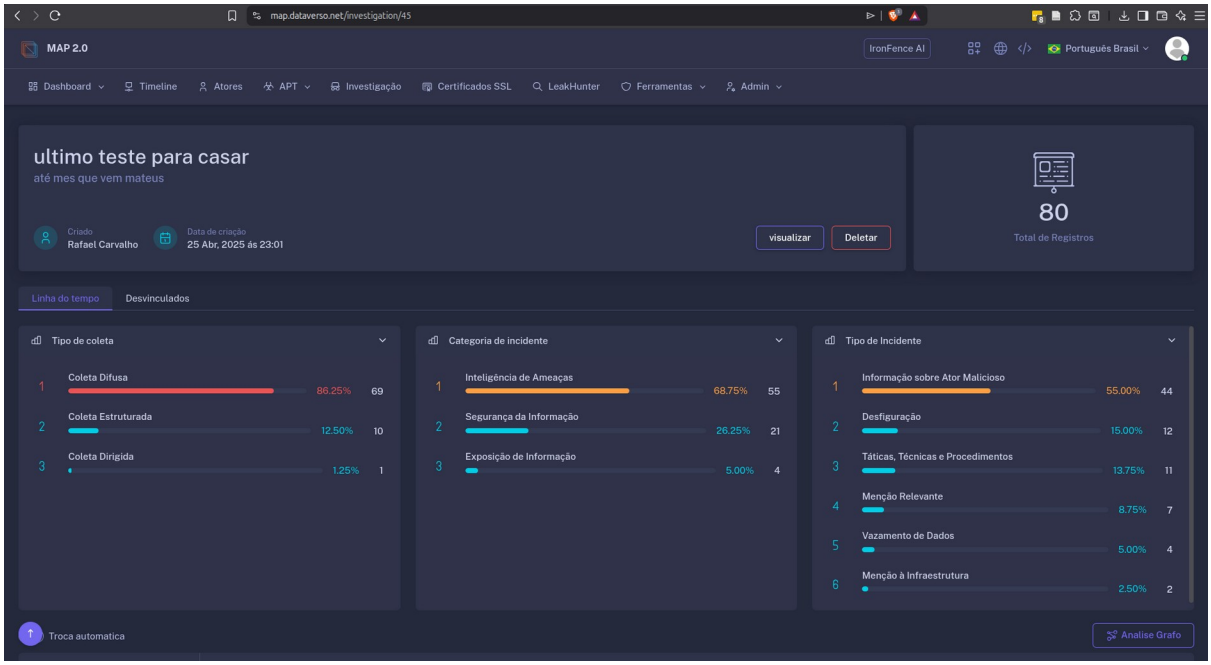
3.30. A solução deve permitir salvar o resultado da pesquisa.



Na tela de pesquisa, temos o botão Exportador, que permite salvar os registros de uma pesquisa.
Ele é orientado pelo filtro de pesquisa (correlacionador) e pode exportar os dados nos formatos CSV, JSON, XML e TAXII/STIX.

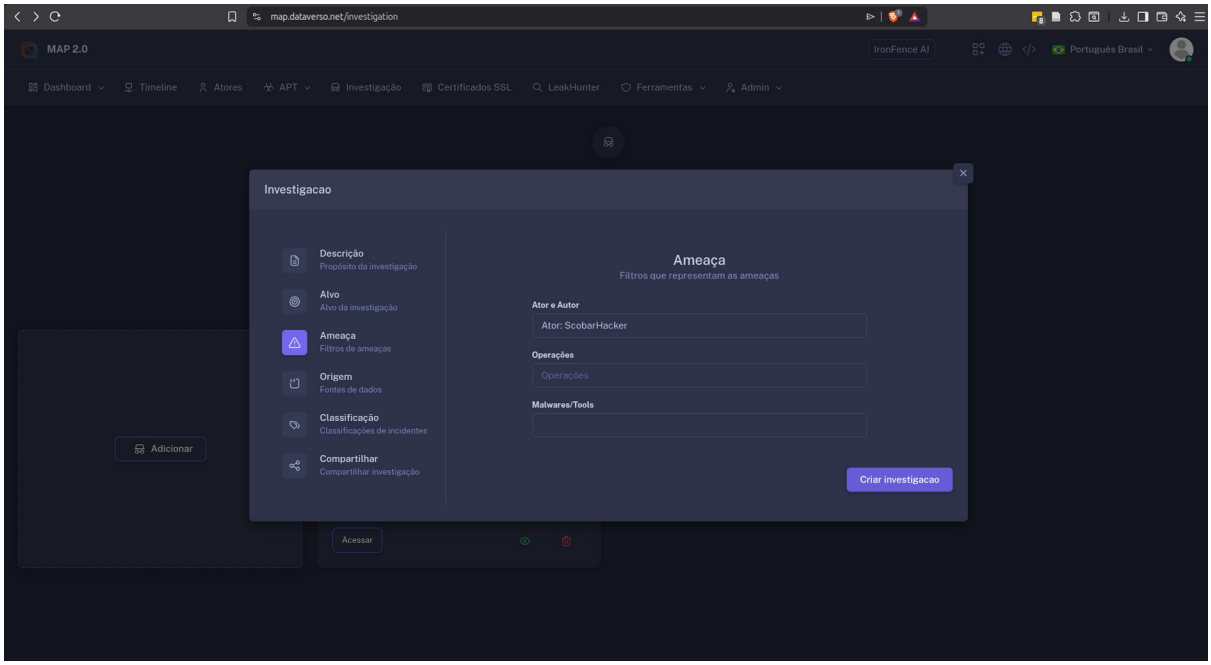
3.31. A solução deve possuir um painel de visualização de todas as pesquisas salvas, possibilitando a execução dessas pesquisas salvas.





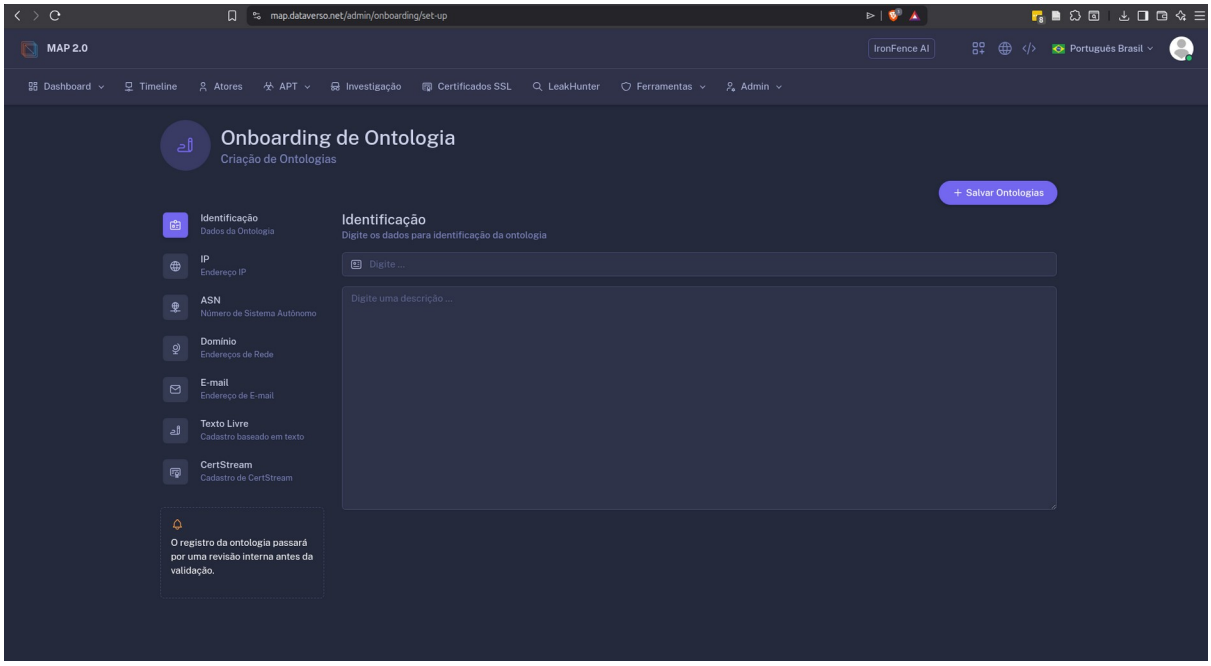
https://map.dataverso.net/investigation

3.32. A solução deve possuir mecanismo que permita que buscas criadas possam ser salvas para uso posterior.



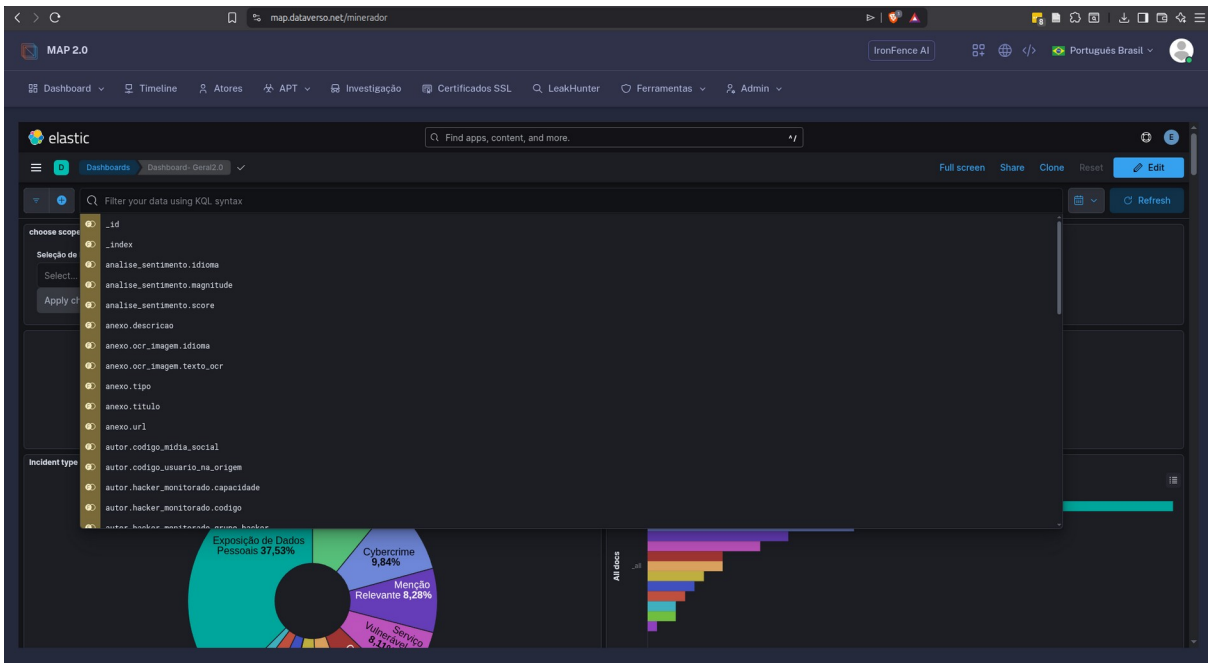
https://map.dataverso.net/investigation

3.33. A solução deve permitir a criação/alteração/exclusão de variáveis na plataforma, possibilitando gerenciamento de termos ou buscas dentro dessa variável.



https://map.dataverso.net/admin/onboarding/set-up

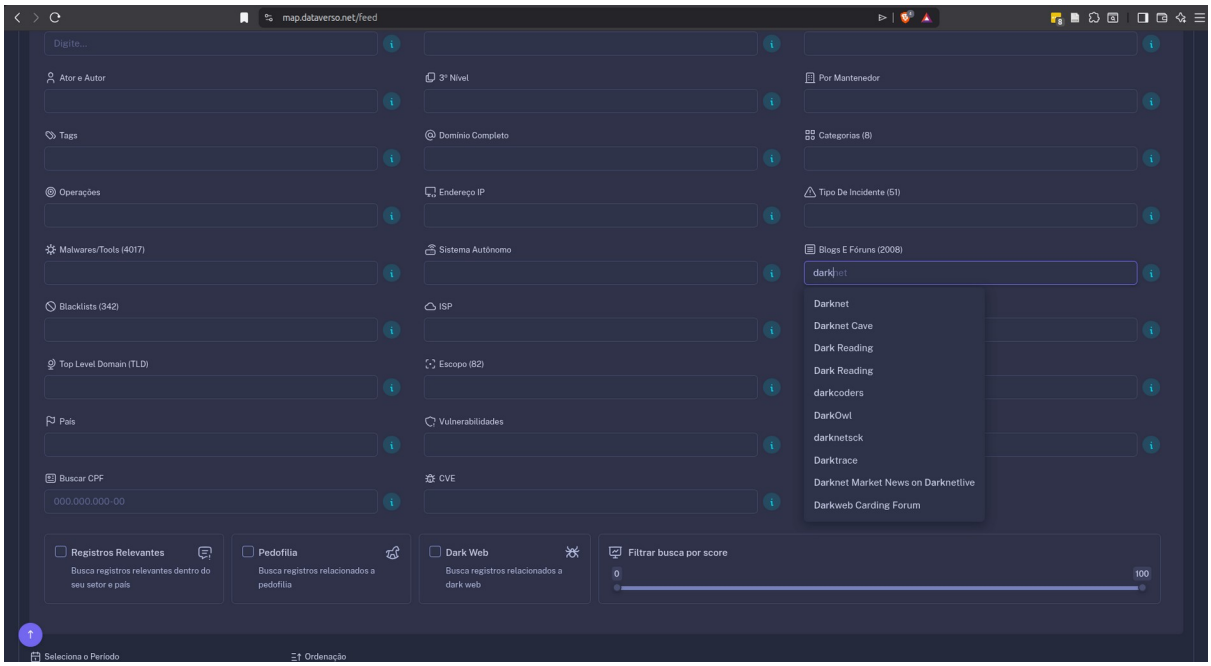
3.34. A ferramenta deve permitir o drill-down das pesquisas utilizando filtros inclusivos e exclusivos;



https://map.dataverso.net/minerador

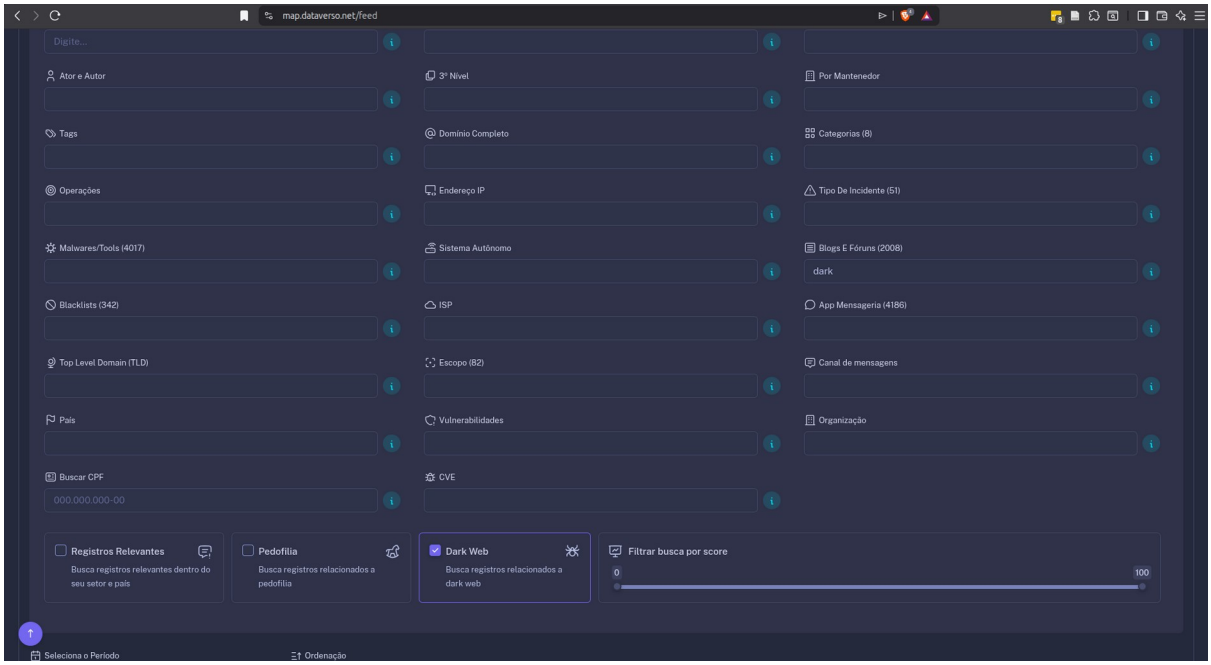
4. MONITORAMENTO DE MARCA, PRODUTOS E EXECUTIVOS

O monitoramento de marca, produtos e executivos envolve rastrear menções online (em redes sociais, fóruns, dark web, etc.) para identificar ameaças como campanhas de difamação, vazamentos de dados ou tentativas de phishing direcionadas. Ferramentas como Brandwatch, Recorded Future ou soluções baseadas em OSINT (Open-Source Intelligence). IA deve ser utilizada para analisar os eventos de forma contextual, detectando anomalias em tempo real e classificando-as por prioridade, com o objetivo de proteger a reputação e identificar ataques direcionados a executivos do Banco (ex.: spear phishing). A seguir os requisitos para monitoramento de marca, produtos e executivos:
4.1. Monitorar menções à marca em tempo real em redes sociais, fóruns, blogs e mídia tradicional.



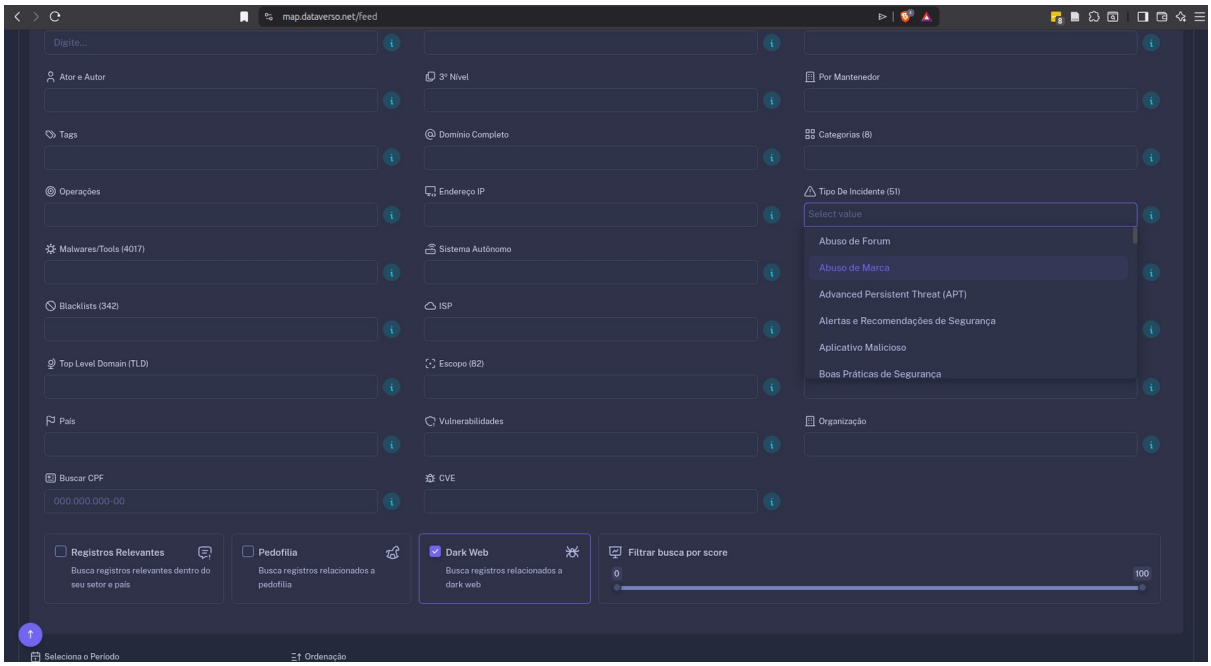
https://map.dataverso.net/feed

4.2. Rastrear a dark web e deep web para identificar vazamentos de dados ou credenciais relacionadas à marca ou executivos.



https://map.dataverso.net/feed

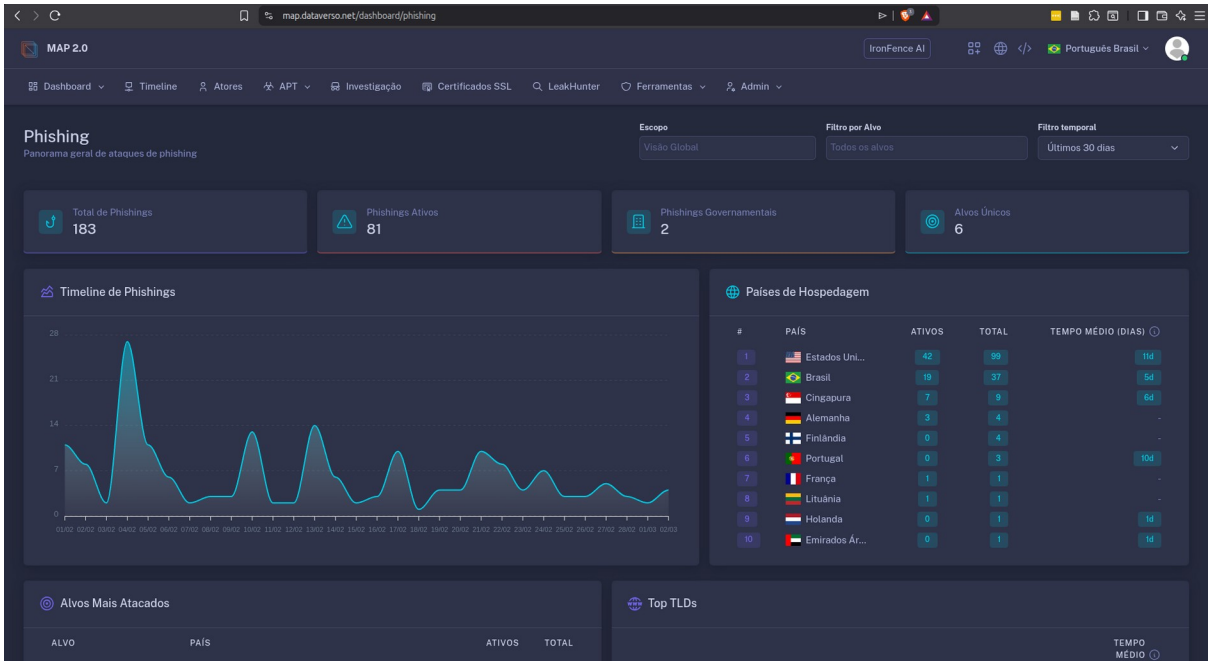
4.3. Detectar campanhas de difamação ou desinformação contra a marca ou executivos.



https://map.dataverso.net/feed

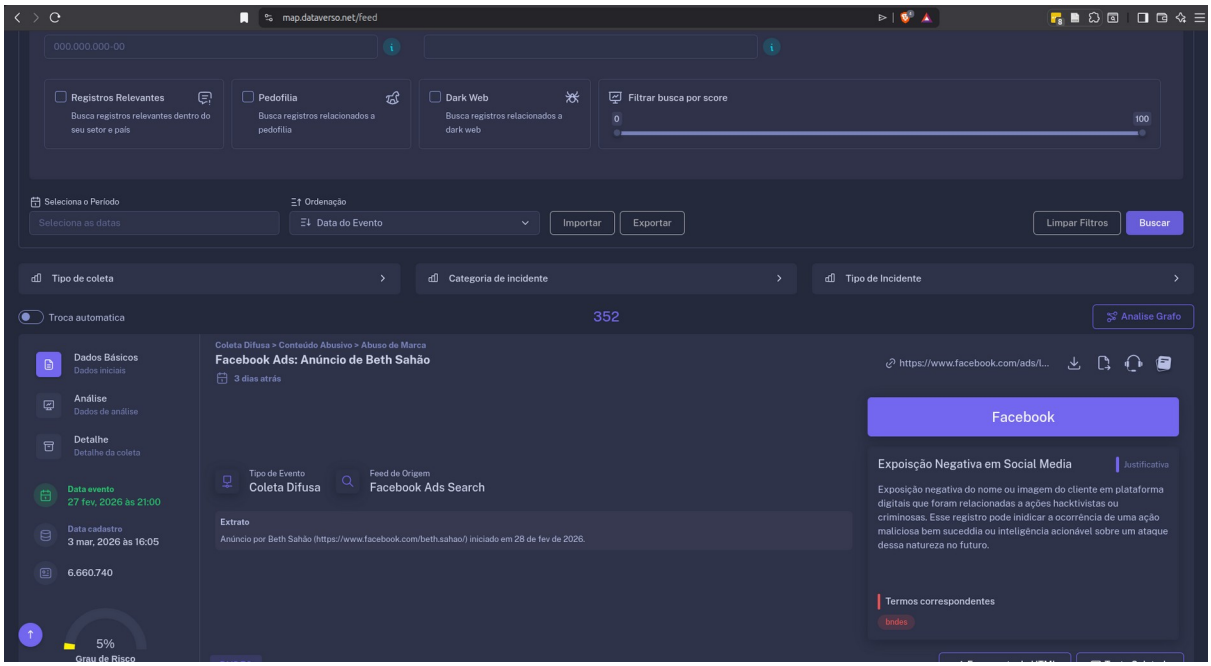
4.4. Identificar atividades voltadas para tentativas de phishing direcionado (spear phishing) contra

executivos.



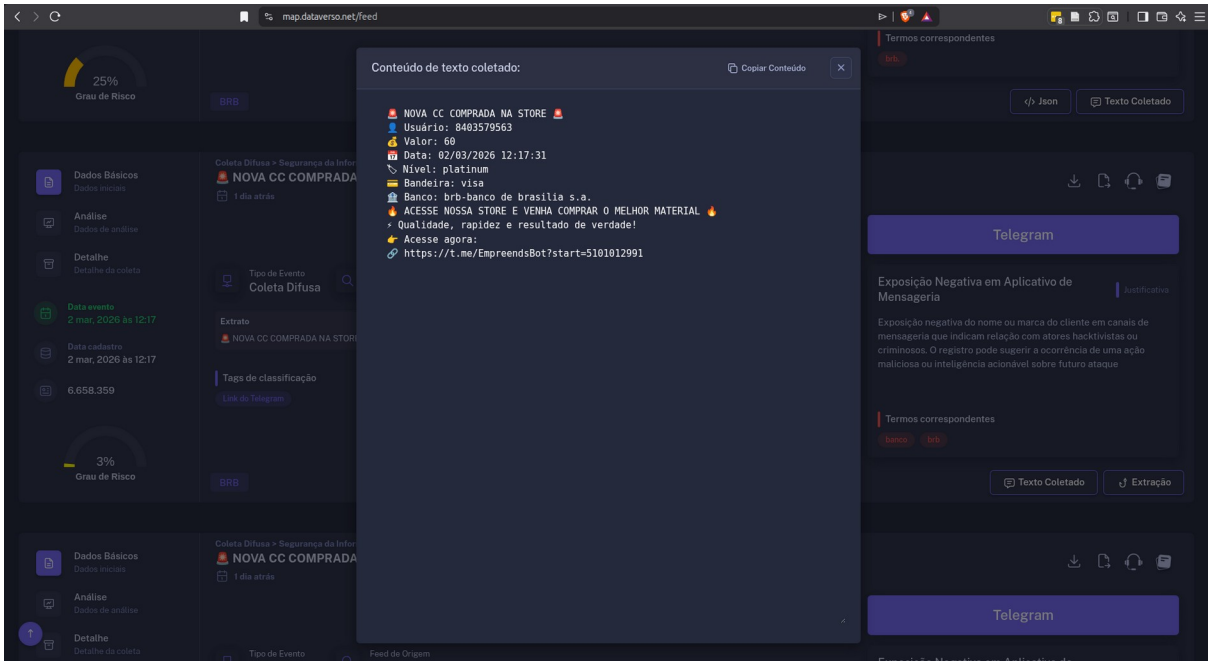
https://map.dataverso.net/dashboard/phishing

4.5. Monitorar perfis falsos ou não autorizados que imitem a marca ou executivos em plataformas digitais.



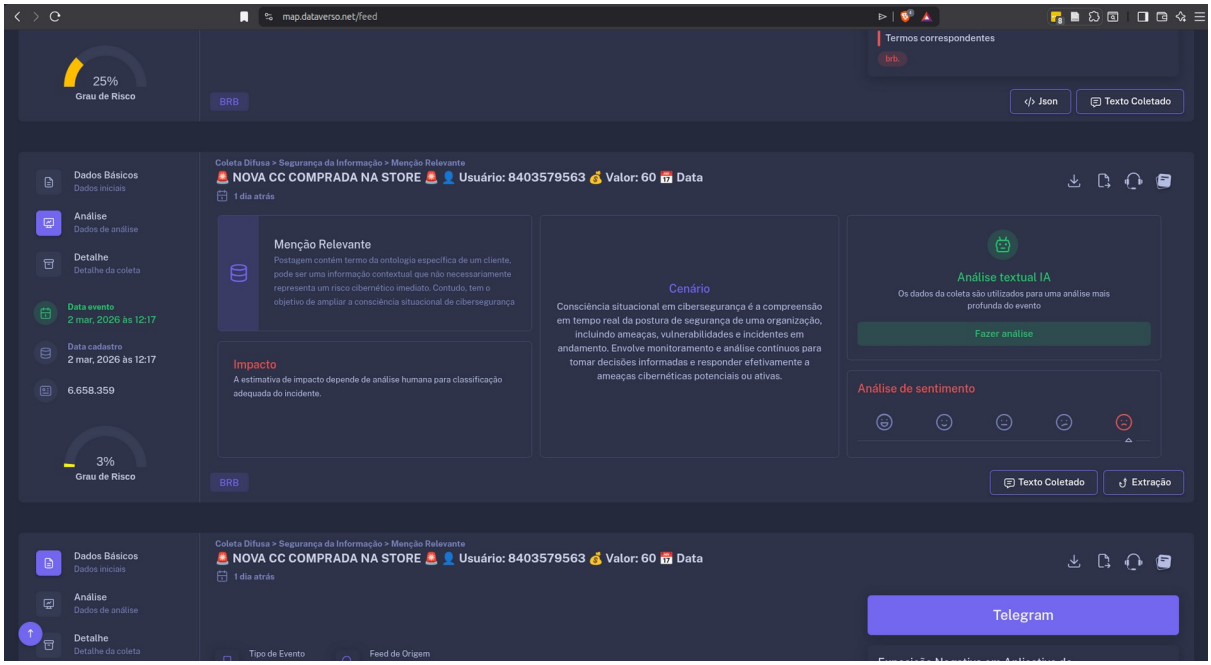
https://map.dataverso.net/feed
Tipo de incidente abuso de marca

4.6. Fornecer alertas em tempo real sobre menções sensíveis ou ameaças à reputação.



https://map.dataverso.net/feed tipo de incidente - exposição de dados financeiros

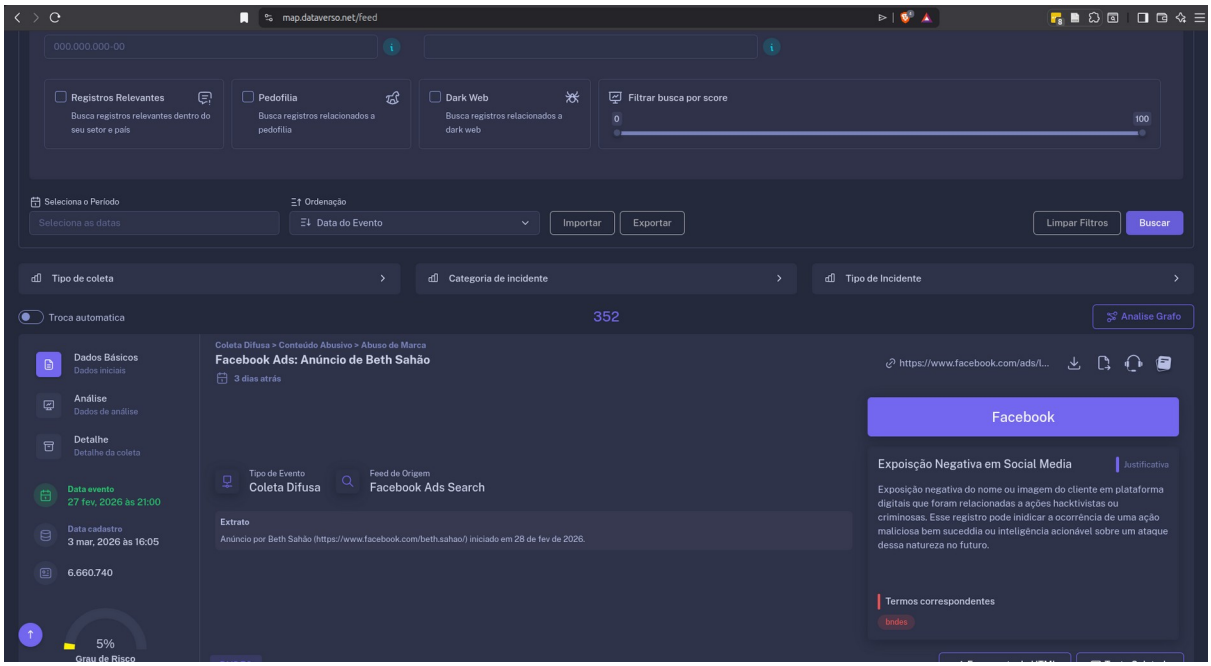
4.7. Analisar contextualmente menções públicas que expressem sentimentos ou tendências negativas, classificando-as conforme o conteúdo transmitido (uso de palavras ofensivas, ameaças, dentre outros).



https://map.dataverso.net/feed

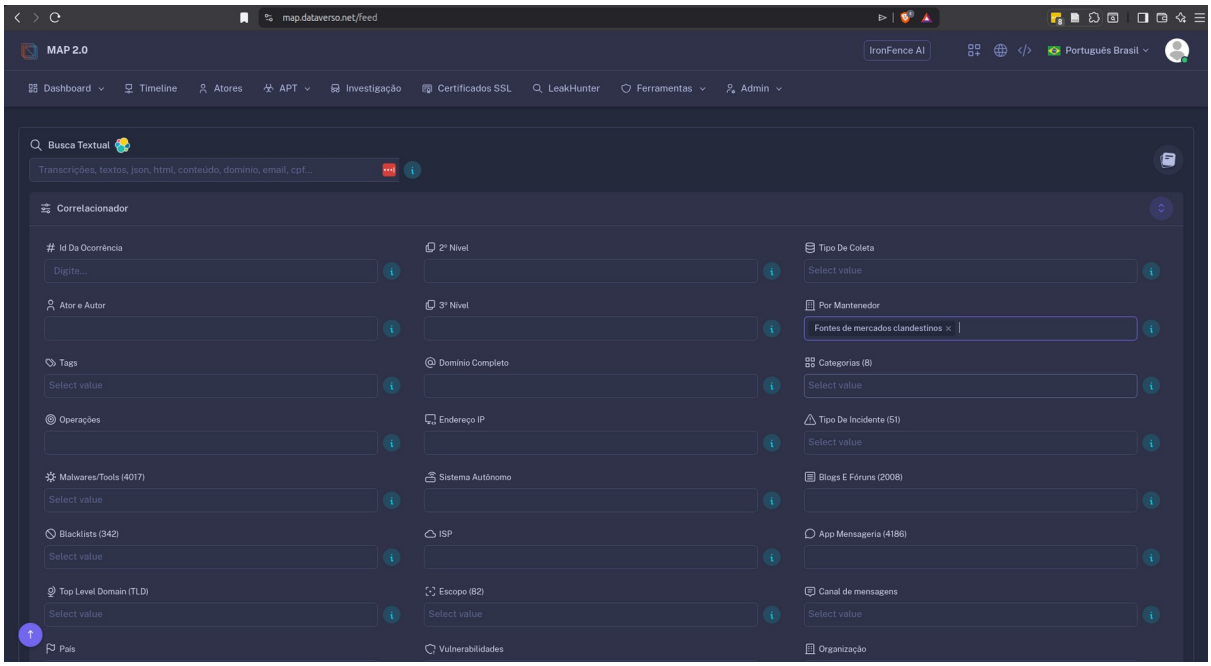
Analise > Análise de Sentimento

4.8. Rastrear uso indevido de logotipos, marcas registradas ou propriedade intelectual.



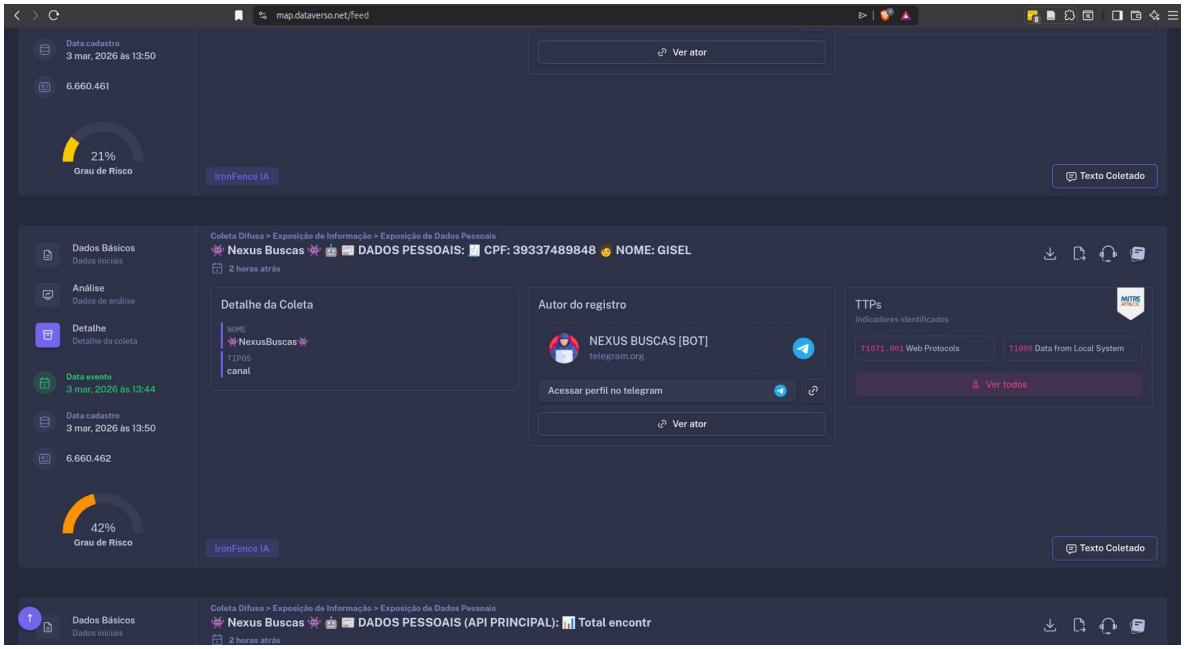
https://map.dataverso.net/feed
Tipo de incidente abuso de marca

4.9. Monitorar marketplaces ilícitos para detectar vendas de dados roubados relacionados à marca.



https://map.dataverso.net/feed

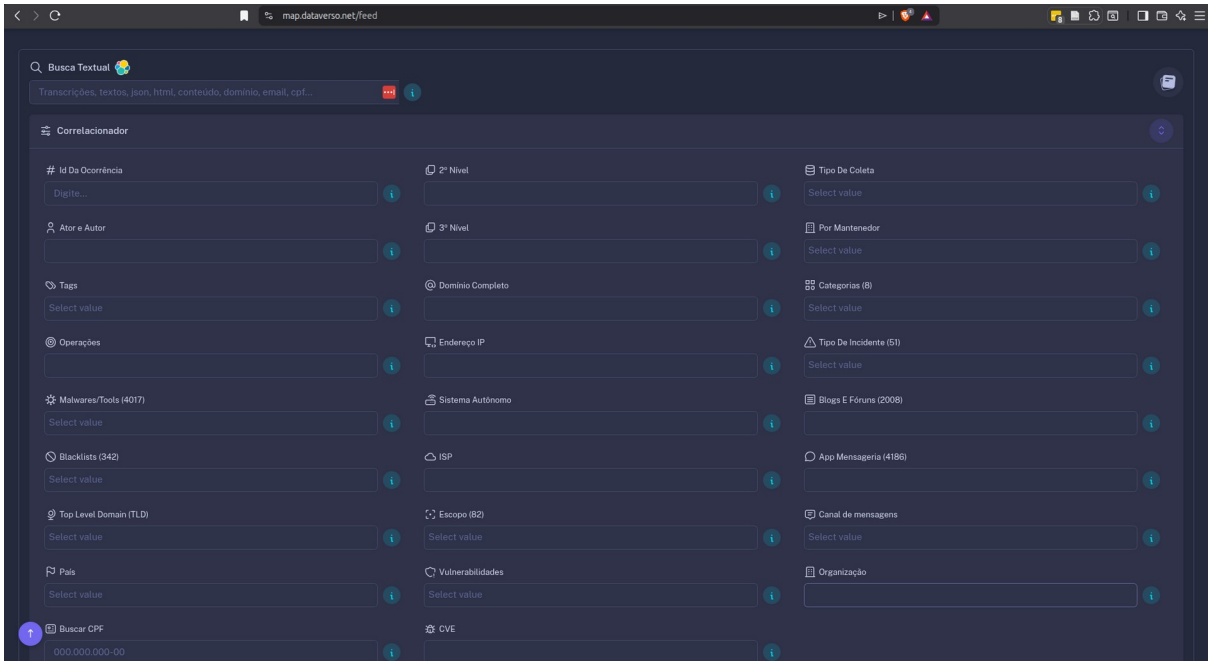
4.10. Fornecer relatórios detalhados sobre atividades suspeitas envolvendo executivos (ex.: doxxing).



https://map.dataverso.net/feed

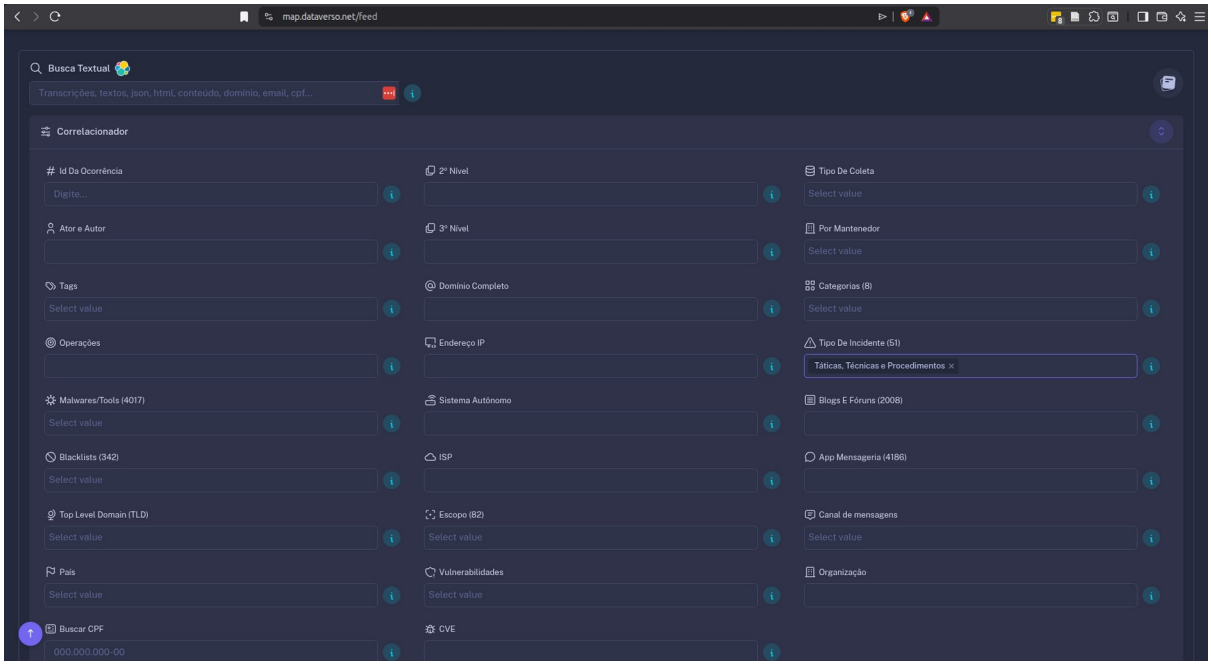
Exposição de dados pessoais

4.11. Utilizar ferramentas de OSINT (Open-Source Intelligence) para coleta de dados públicos.



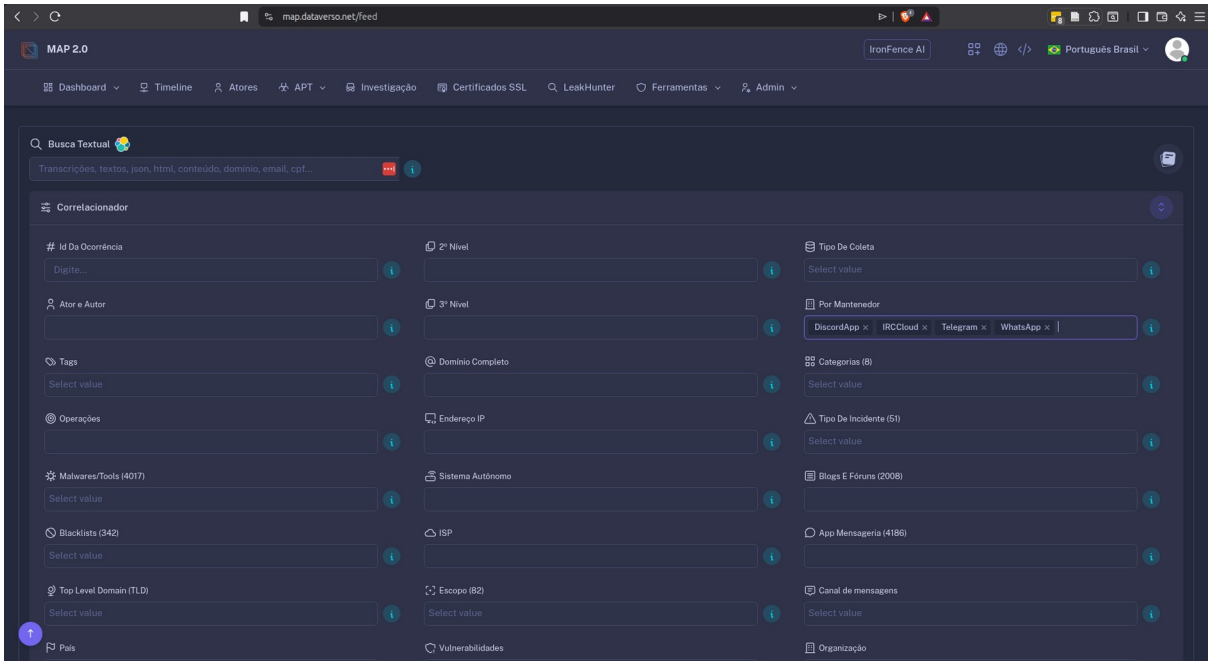
https://map.dataverso.net/feed

4.12. Identificar tentativas de engenharia social direcionadas a executivos ou funcionárioschave.



https://map.dataverso.net/feed
Tipo de incidente TTP

4.13. Monitorar plataformas de mensagens instantâneas (ex.: Telegram, Discord) para ameaças à marca.

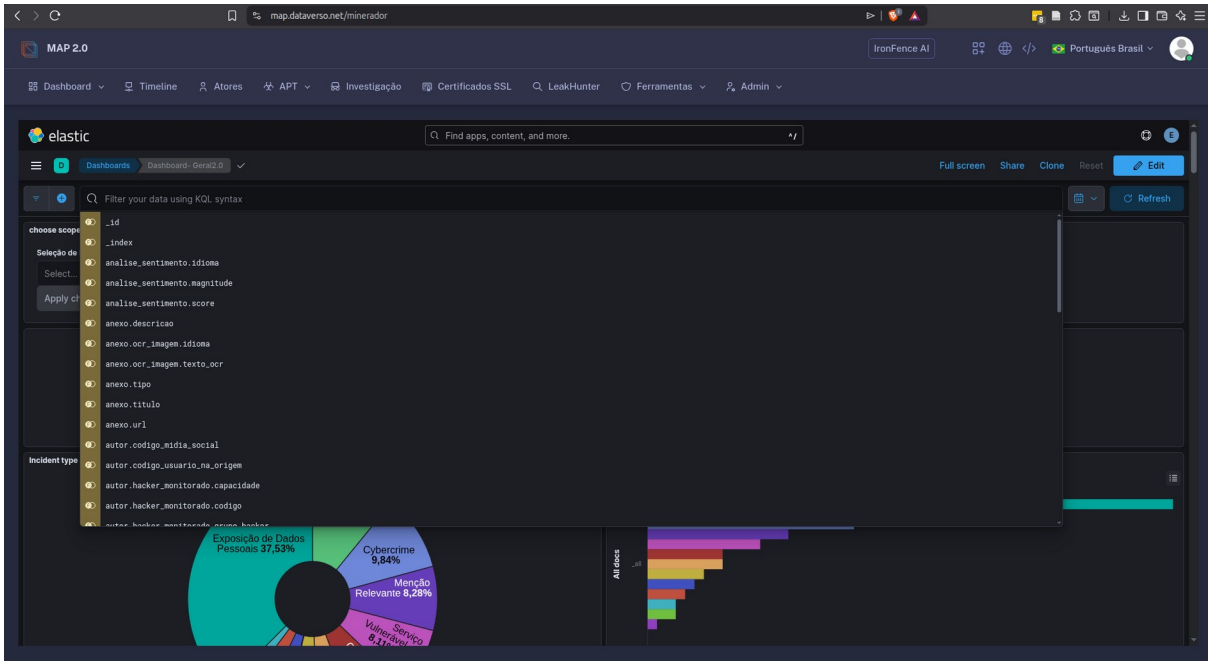


https://map.dataverso.net/feed

4.14. Garantir anonimato nas operações de monitoramento para proteger o contratante.

A plataforma garante o anonimato nas operações de monitoramento por meio de uma infraestrutura dedicada, integralmente operada pela plataforma MAP. O processo de coleta utiliza avatares próprios com identidades e perfis virtuais criados exclusivamente para o monitoramento em fóruns, redes sociais, grupos de mensagens, marketplaces e ambientes da deep e dark web. Toda a comunicação é realizada através de servidores virtuais próprios, links de conexão dedicados e camadas de proxies, garantindo que nenhuma operação de coleta possa ser rastreada ou associada ao Banco do Nordeste. Essa arquitetura assegura que a identidade do CONTRATANTE permaneça protegida em todas as etapas do monitoramento, desde a coleta até o armazenamento dos dados.

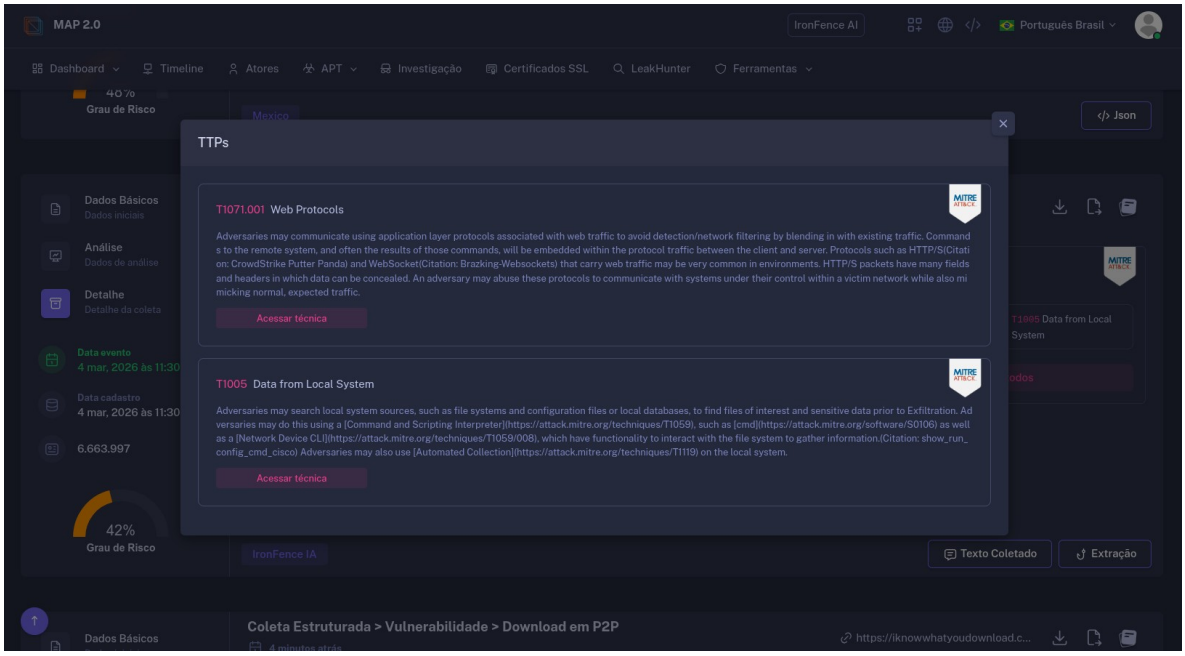
4.15. Fornecer painéis interativos para visualização de dados de monitoramento de marca.



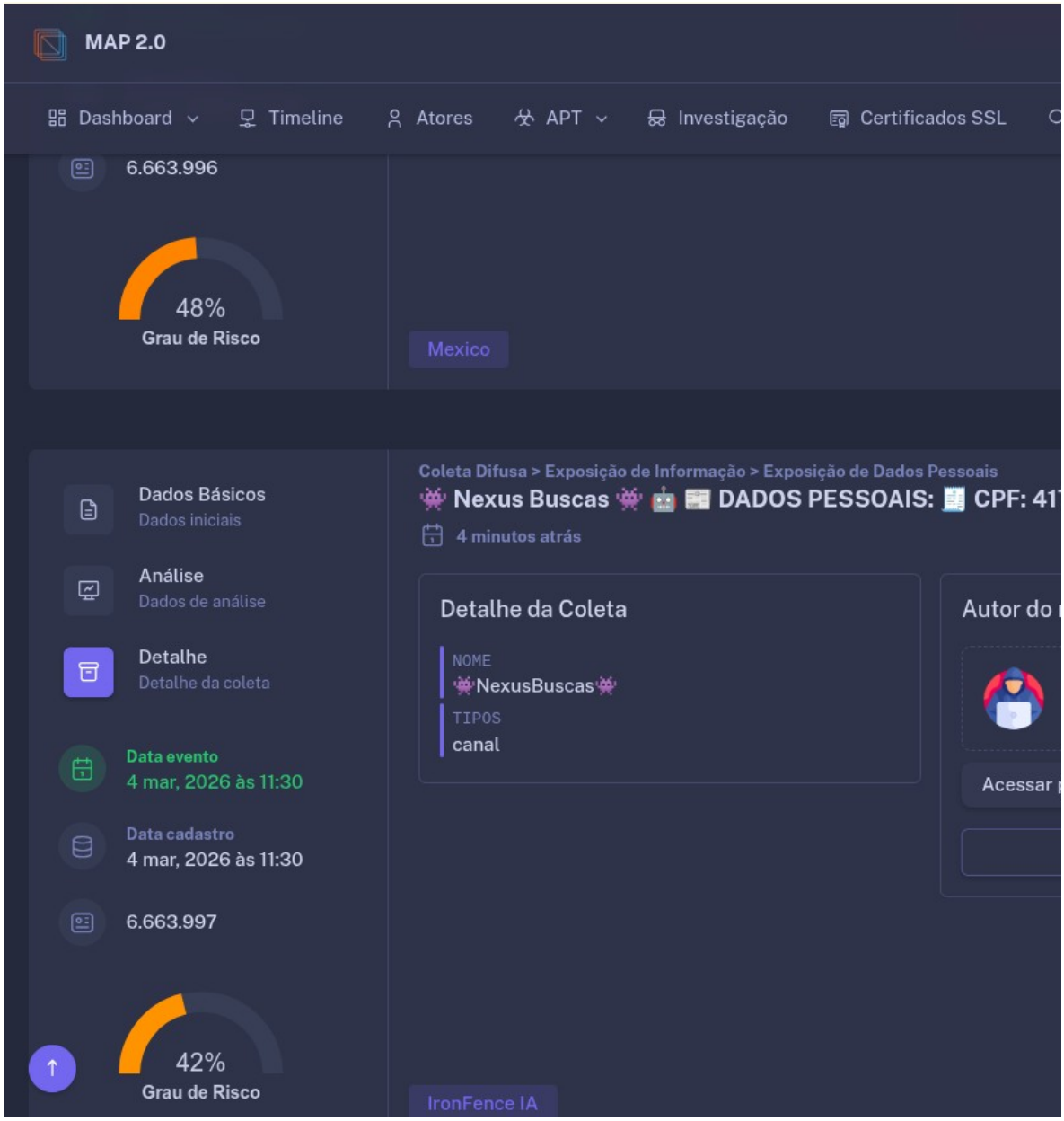
https://map.dataverso.net/minerador

5. CLASSIFICAÇÃO E PRIORIZAÇÃO DE RISCOS

A solução deve providenciar a classificação de riscos com base em probabilidade, impacto e criticidade dos ativos envolvidos. A priorização dos riscos pode ser automatizada com IA, que analisa dados históricos e contexto (ex.: vulnerabilidades críticas em sistemas expostos).
5.1. Utilizar frameworks reconhecidos (ex.: MITRE ATT&CK, NIST) para classificação de riscos.



5.2. Utilizar ferramentas (ex.: RiskLens ou métodos qualitativos/quantitativos) para priorizar os riscos.

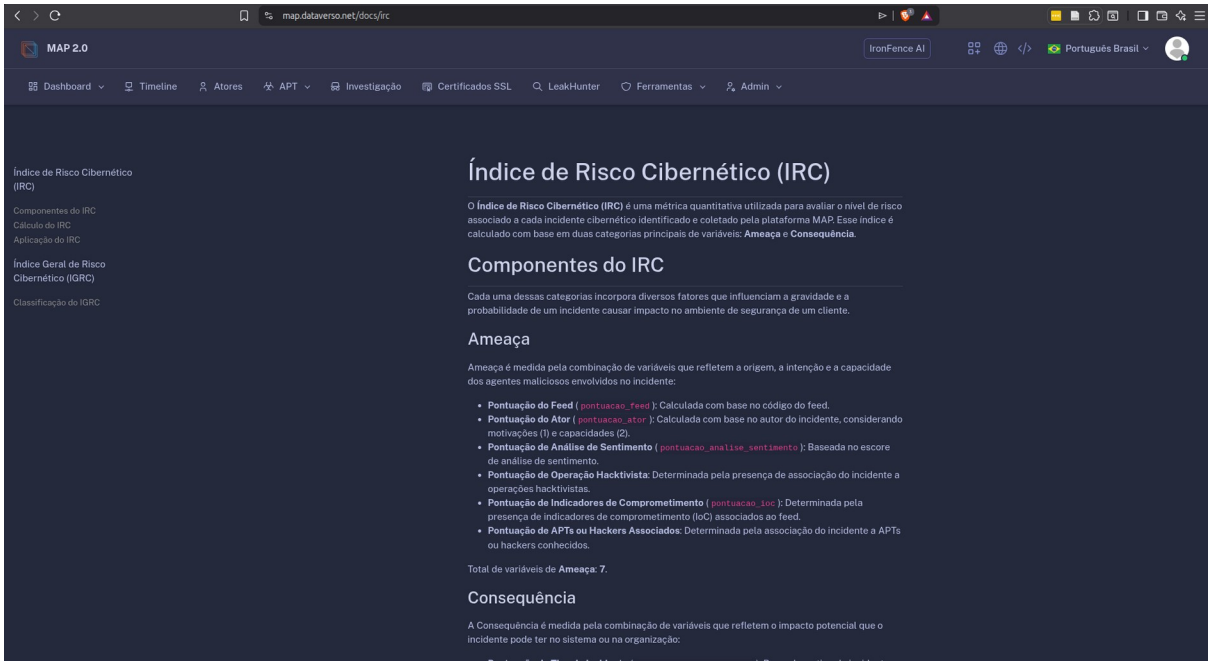


5.3. Avaliar riscos com base em probabilidade, impacto e criticidade dos ativos.

5.4. Priorizar ameaças com base em contexto organizacional (ex.: setor, localização, tamanho).

Há uma estratégia avançada para tratamento de riscos, conforme descrito na imagem acima e no link da plataforma: https://map.dataverso.net/docs/irc

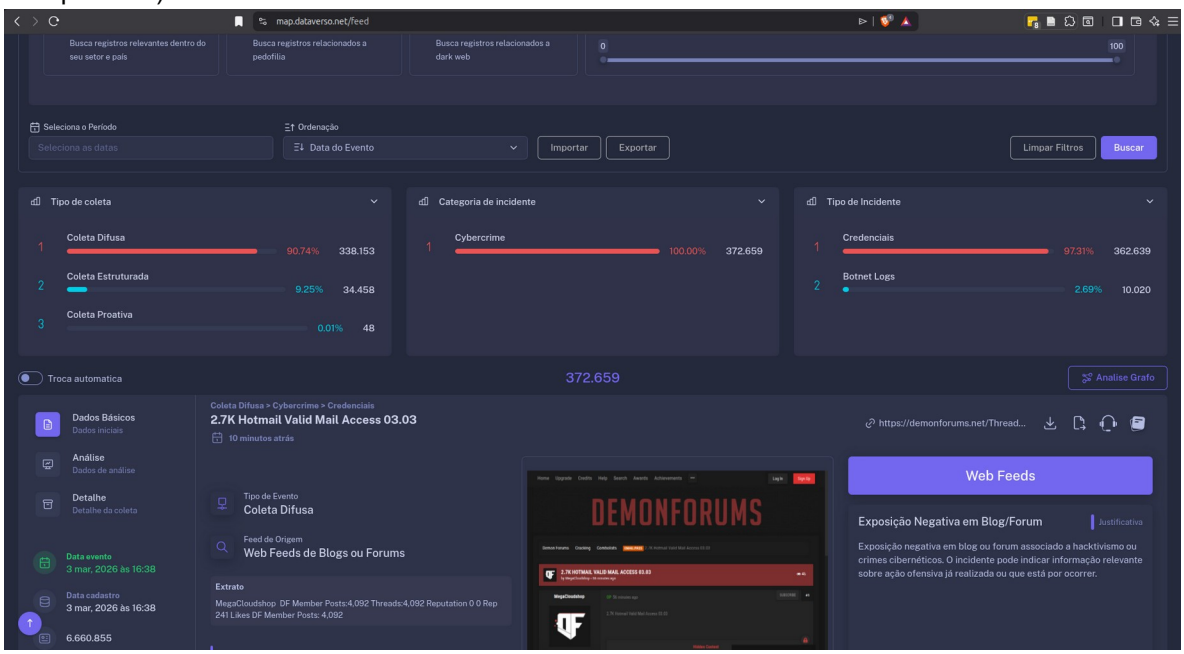
5.5. Fornecer scores de risco quantitativos e qualitativos para cada ameaça identificada.



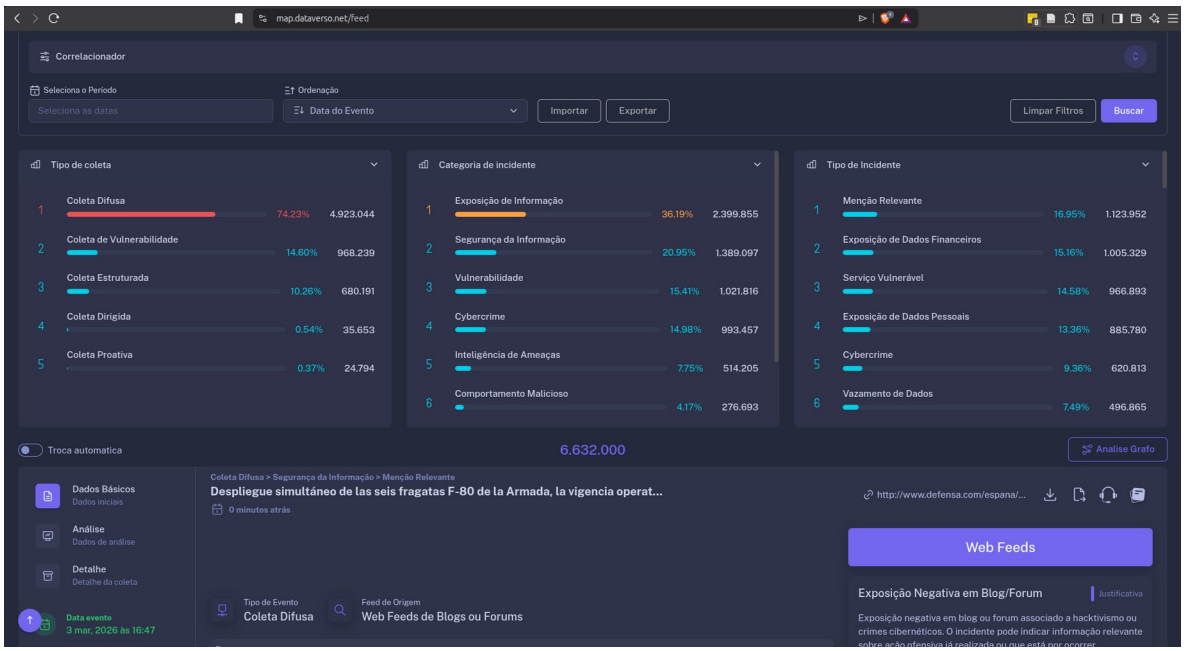
https://map.dataverso.net/docs/irc

5.6. Atualizar a priorização de riscos em tempo real com base em novos dados de inteligência.

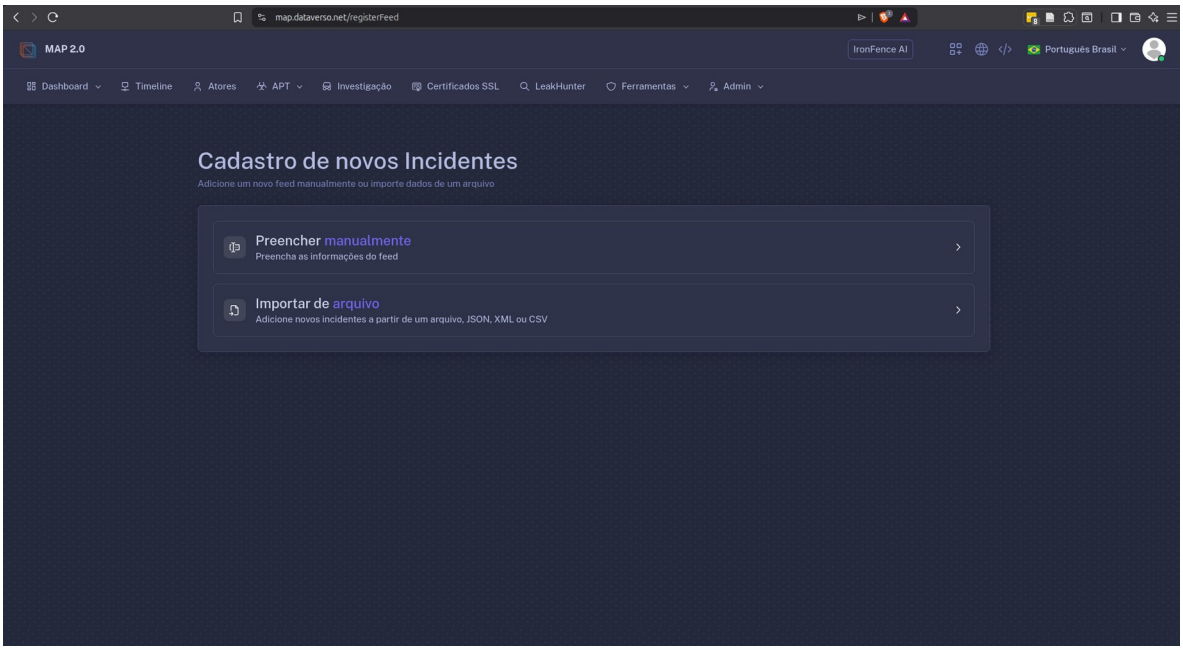
5.7. Identificar riscos específicos para fraudes financeiras, como BEC (Business Email Compromise).



5.8. Classificar ameaças por tipo (ex.: malware, phishing, insider threats).

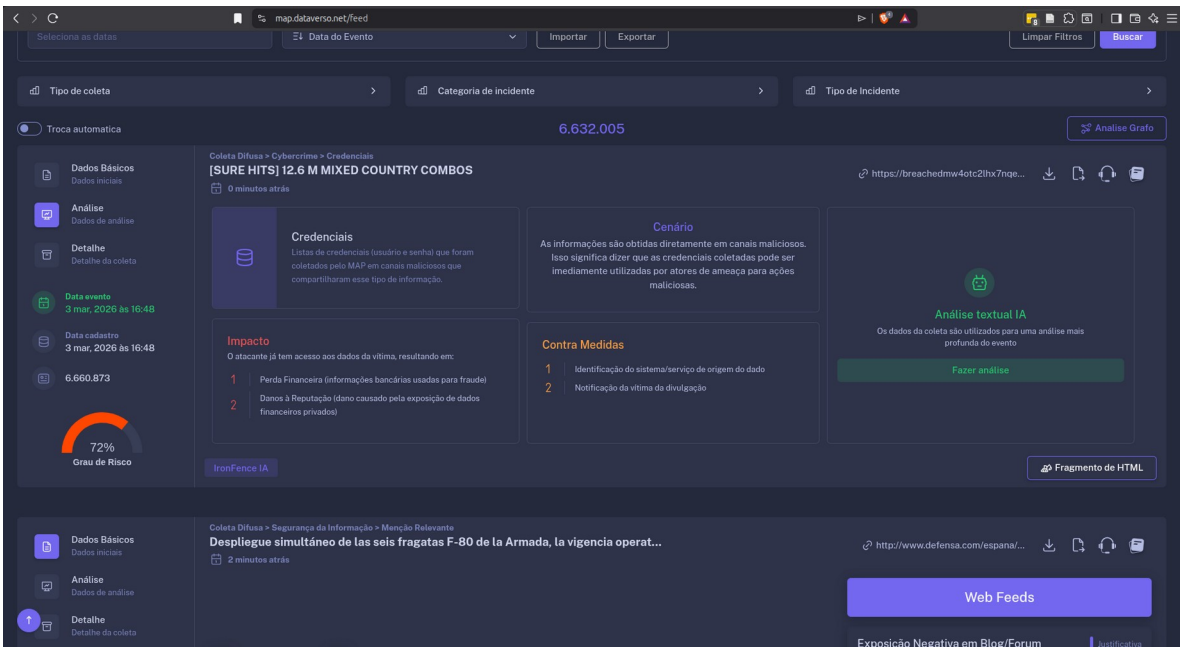


5.9. Integrar dados de inteligência interna do contratante na avaliação de riscos.

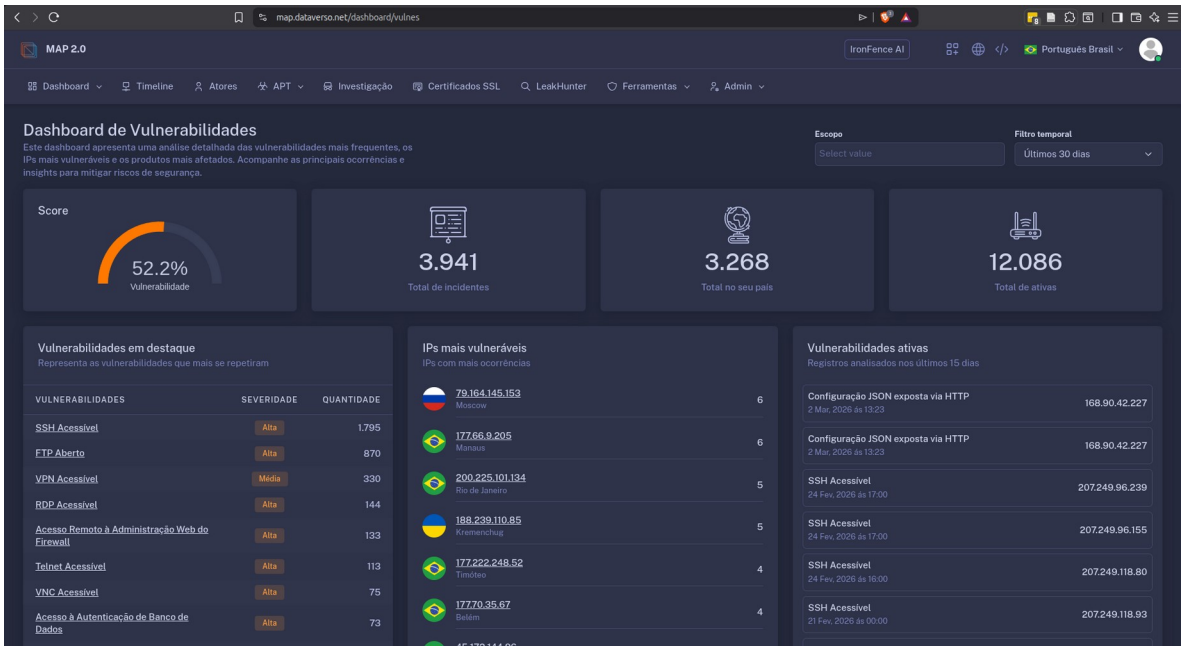


https://map.dataverso.net/registerFeed

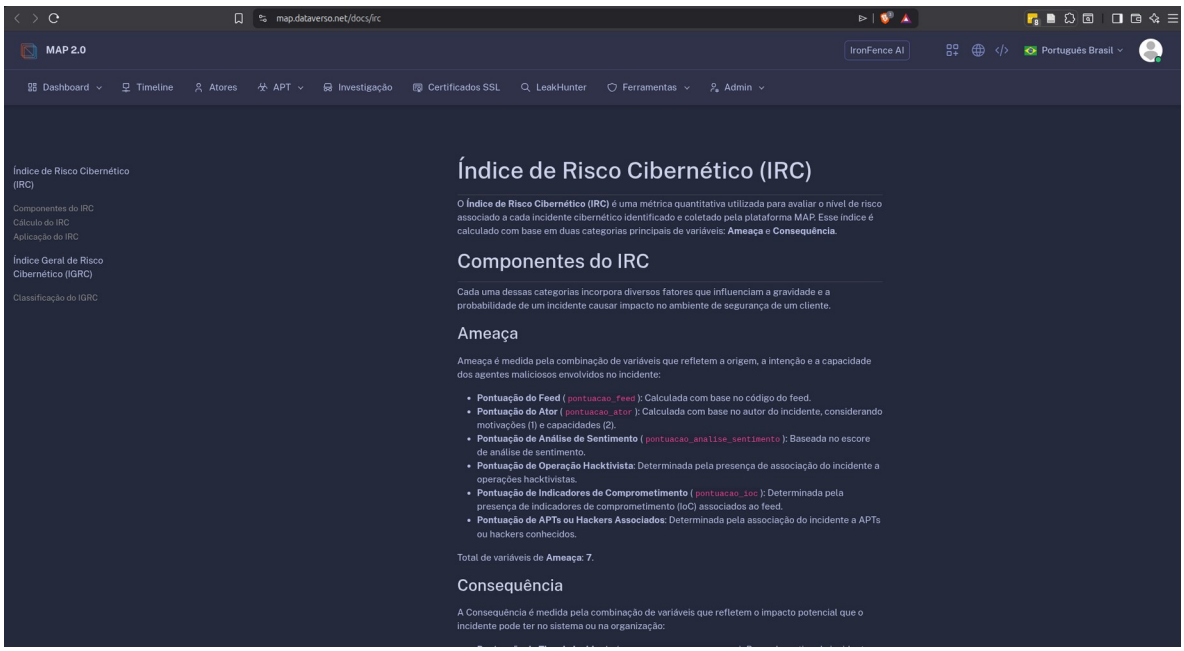
5.10. Fornecer relatórios de riscos com recomendações acionáveis para mitigação.



5.11. Priorizar riscos com base em vulnerabilidades conhecidas em sistemas do contratante.

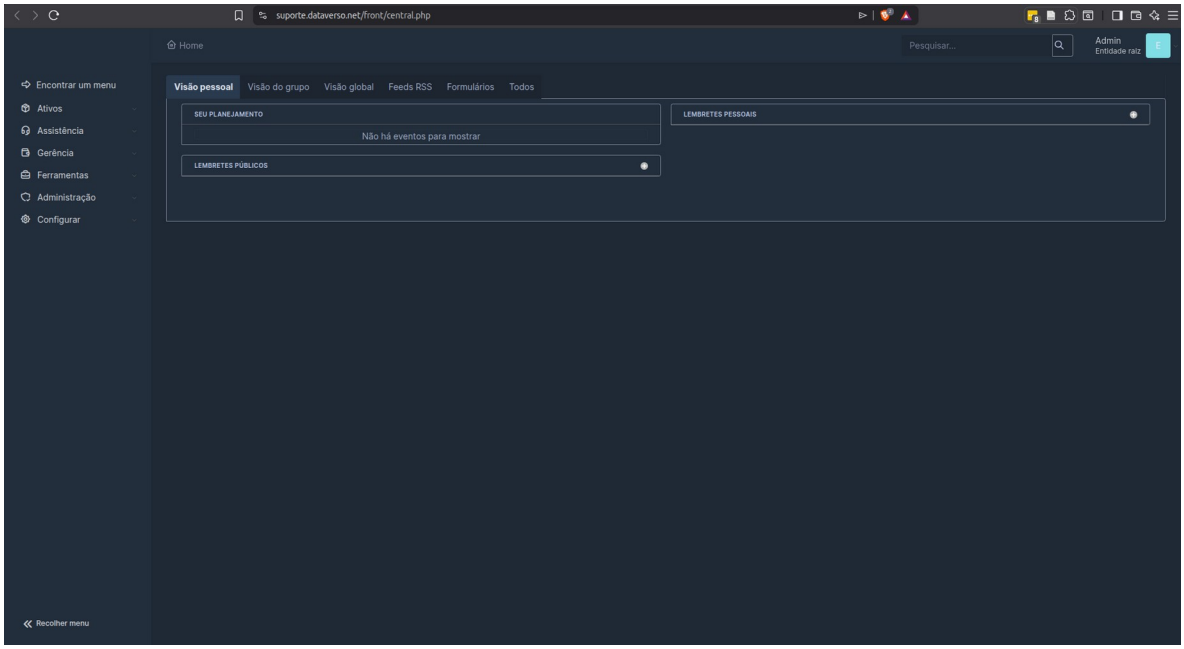


5.12. Garantir transparência na metodologia de classificação de riscos.



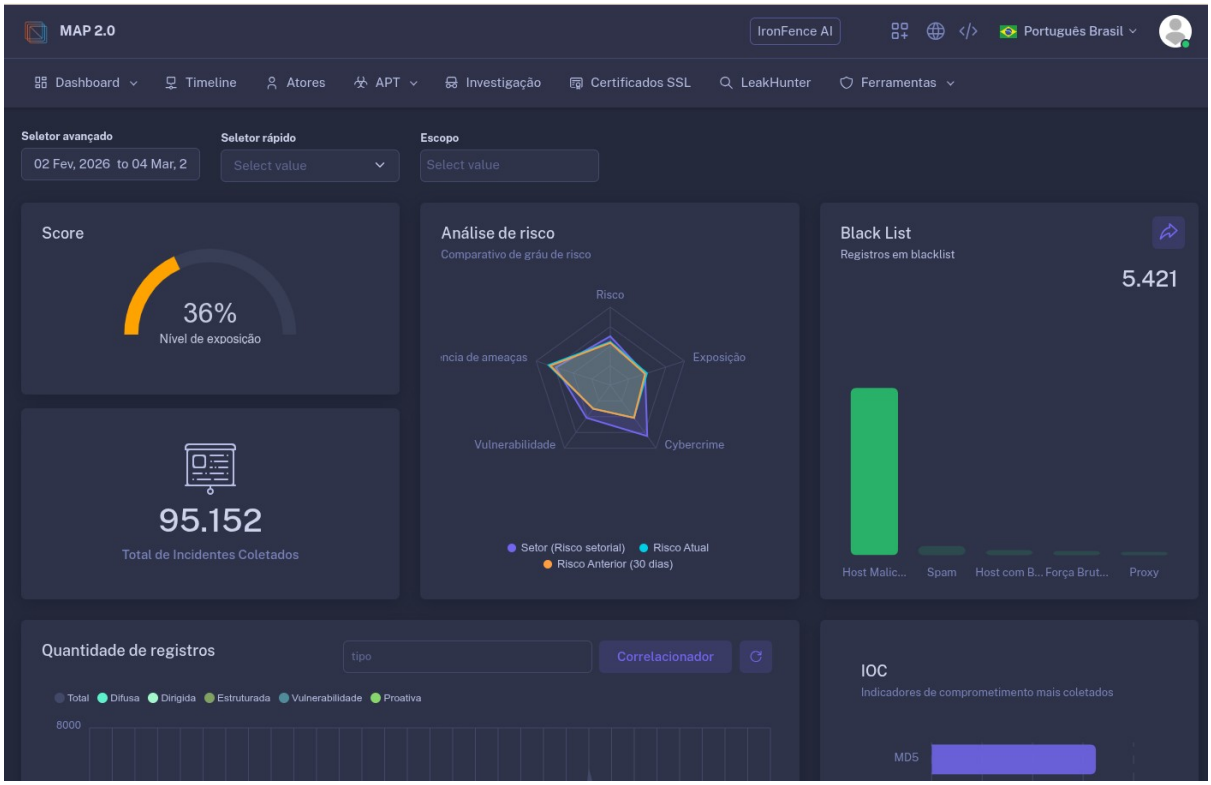
https://map.dataverso.net/docs/irc

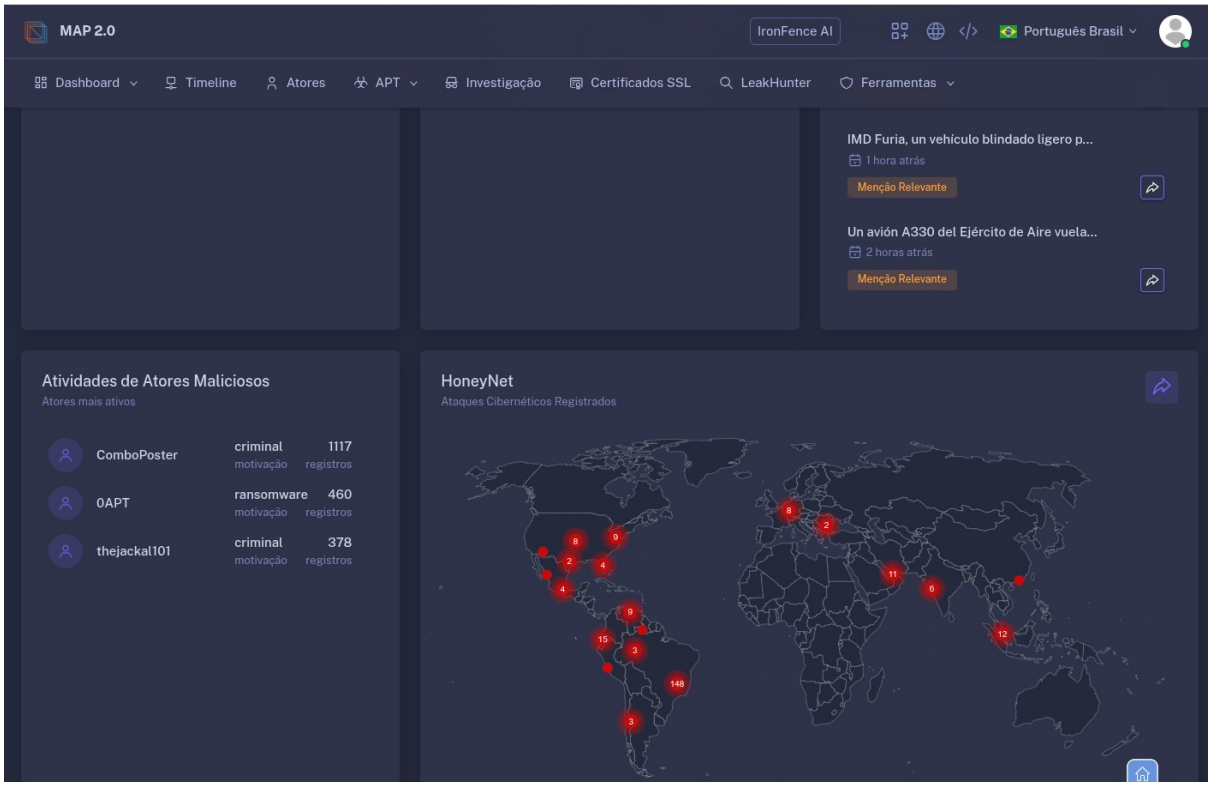
5.13. Oferecer suporte para revisão periódica da matriz de riscos.



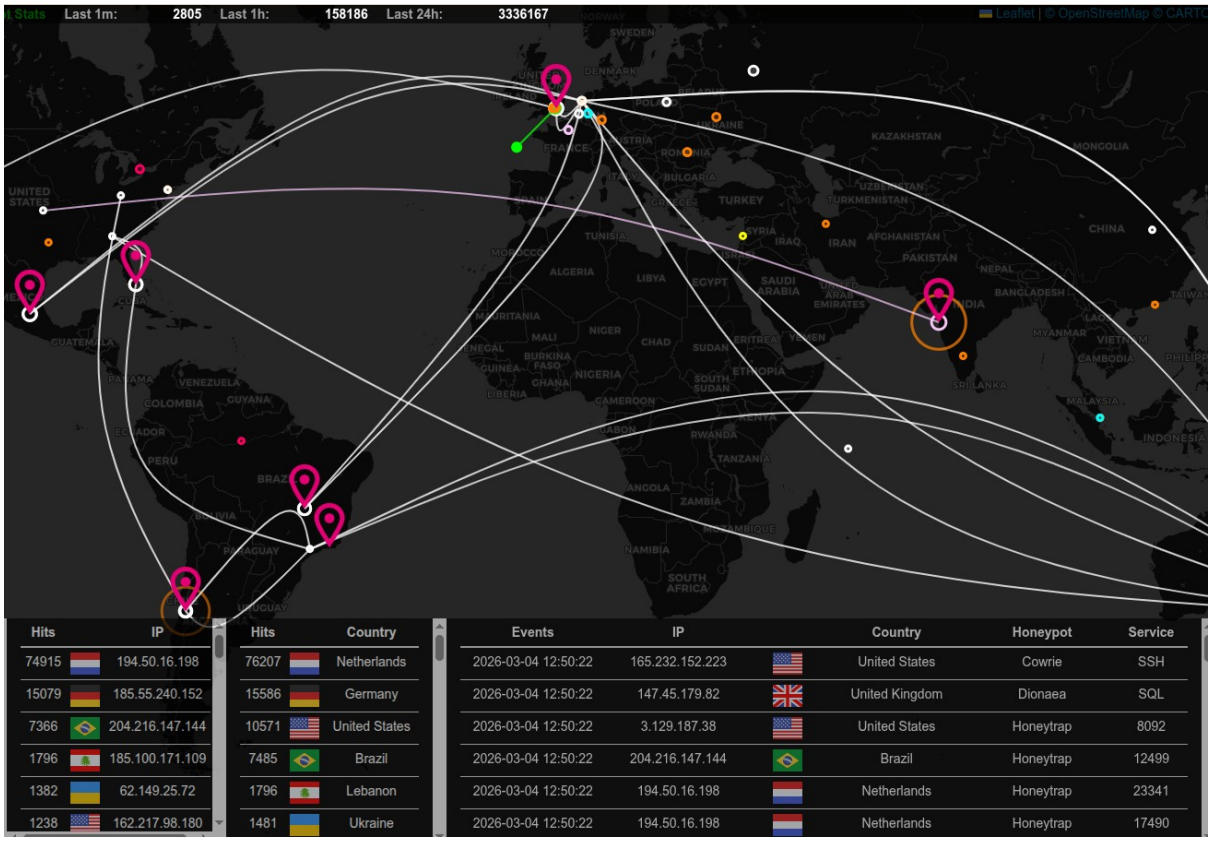
https://suporte.dataverso.net/front/central.php

5.14. Identificar riscos emergentes com base em tendências globais de cibersegurança.



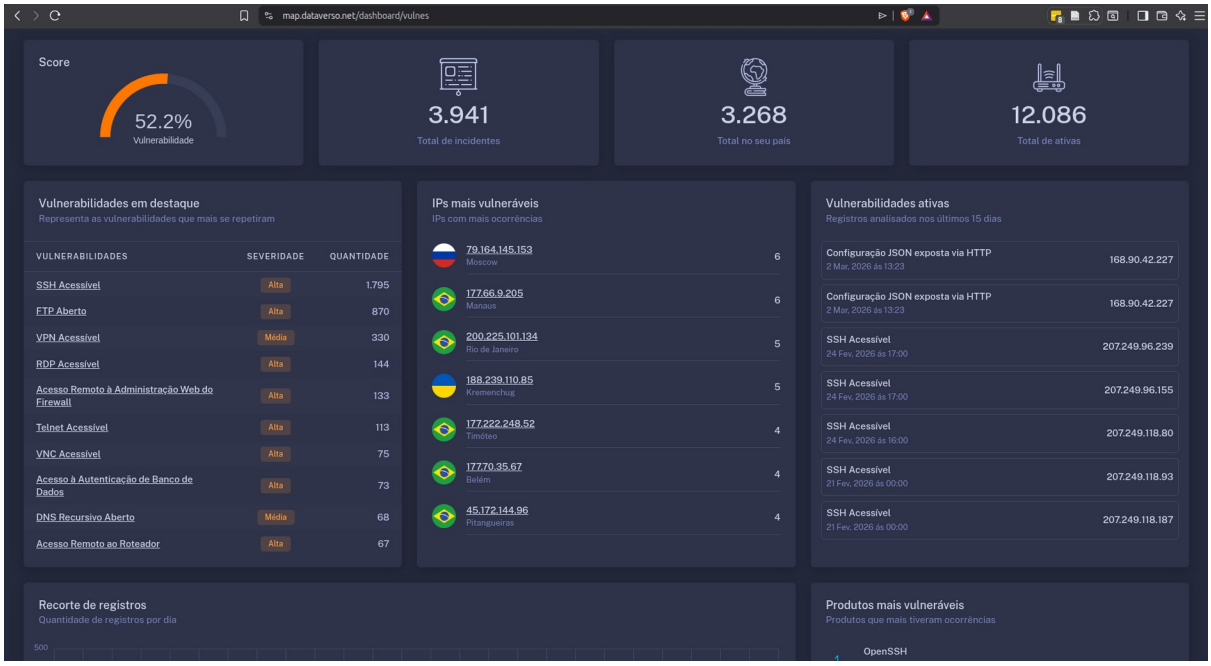


https://map.dataverso.net/dashboard



https://map.dataverso.net/panorama/map

5.15. Fornecer análise de impacto potencial de fraudes em operações e reputação.



https://map.dataverso.net/dashboard/vulnes

6. UTILIZAÇÃO DE IA PARA CLASSIFICAÇÃO DE AMEAÇAS

6.1. Utilizar modelos de aprendizado de máquina (ML) para detectar padrões de ameaças em tempo real.

A plataforma MAP emprega uma abordagem híbrida que combina três camadas de detecção: (1) regras e expressões regulares para identificação determinística de padrões conhecidos como credenciais, cartões, CPFs e hashes; (2) modelos de Machine Learning supervisionados e não supervisionados para classificação automática de ameaças e detecção de anomalias; e (3) IA avançada com Large Language Models (LLM) para análise contextual, processamento de linguagem natural e geração de relatórios inteligentes.

6.2. Empregar processamento de linguagem natural (PLN) para analisar comunicações maliciosas (ex.: e-mails de phishing).

Modelos de PLN analisam textos de e-mails, mensagens e postagens para identificar linguagem maliciosa, tentativas de phishing e engenharia social em múltiplos idiomas.

6.3. Treinar modelos de IA com dados históricos de fraudes relevantes ao setor do contratante.

Os modelos são treinados com datasets históricos de fraudes e ameaças do setor financeiro, incluindo dados contextualizados de incidentes anteriores.

6.4. Reduzir falsos positivos por meio de algoritmos de IA otimizados.

O pipeline híbrido de regras + ML + LLM reduz falsos positivos progressivamente, pois cada camada refina a classificação da anterior.

6.5. Fornecer explicabilidade (explainable AI) para decisões de classificação de ameaças.

Os relatórios gerados por IA incluem explicações detalhadas sobre o motivo da classificação de cada ameaça, permitindo auditoria das decisões.

6.6. Atualizar continuamente os modelos de IA com novos dados de inteligência.

Os modelos são atualizados continuamente com novos dados de inteligência coletados pela plataforma, mantendo a eficácia diante de ameaças emergentes.

6.7. Utilizar IA para correlacionar dados de fontes díspares (ex.: logs, OSINT, dark web).

A IA correlaciona automaticamente dados de fontes díspares — OSINT, dark web, redes sociais, logs e feeds de ameaças — para identificar campanhas coordenadas.

6.8. Implementar IA para prever campanhas de fraude com base em tendências.

Algoritmos preditivos analisam padrões e tendências para antecipar campanhas de fraude antes de sua execução completa.

6.9. Garantir que os modelos de IA sejam auditáveis e conformes com regulamentações.

Os modelos são auditáveis, com registros de decisões e metodologia documentada.

6.10. Fornecer relatórios sobre a eficácia da IA na detecção de ameaças.

Relatórios periódicos sobre métricas de eficácia da IA.

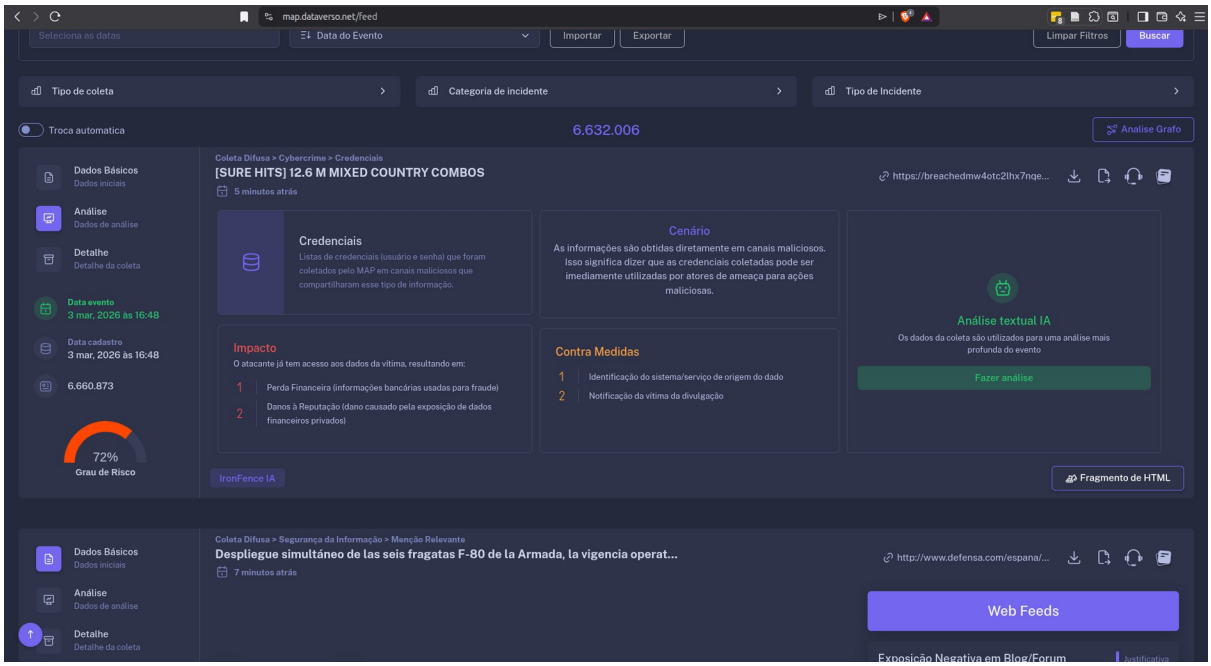
6.11. Utilizar IA para identificar ameaças de baixa visibilidade (ex.: ataques de cadeia de suprimentos).
Modelos de detecção de anomalias identificam ameaças de baixa visibilidade, como ataques de cadeia de suprimentos e movimentações laterais de APTs.

6.12. Integrar IA com ferramentas de visualização para facilitar a análise de ameaças.
Os resultados da IA são integrados diretamente aos dashboards e painéis de visualização da plataforma, facilitando a análise pelas equipes de segurança.

6.13. Garantir que os dados usados para treinar IA respeitem privacidade e conformidade.
Os dados utilizados para treinamento passam por processos de anonimização.

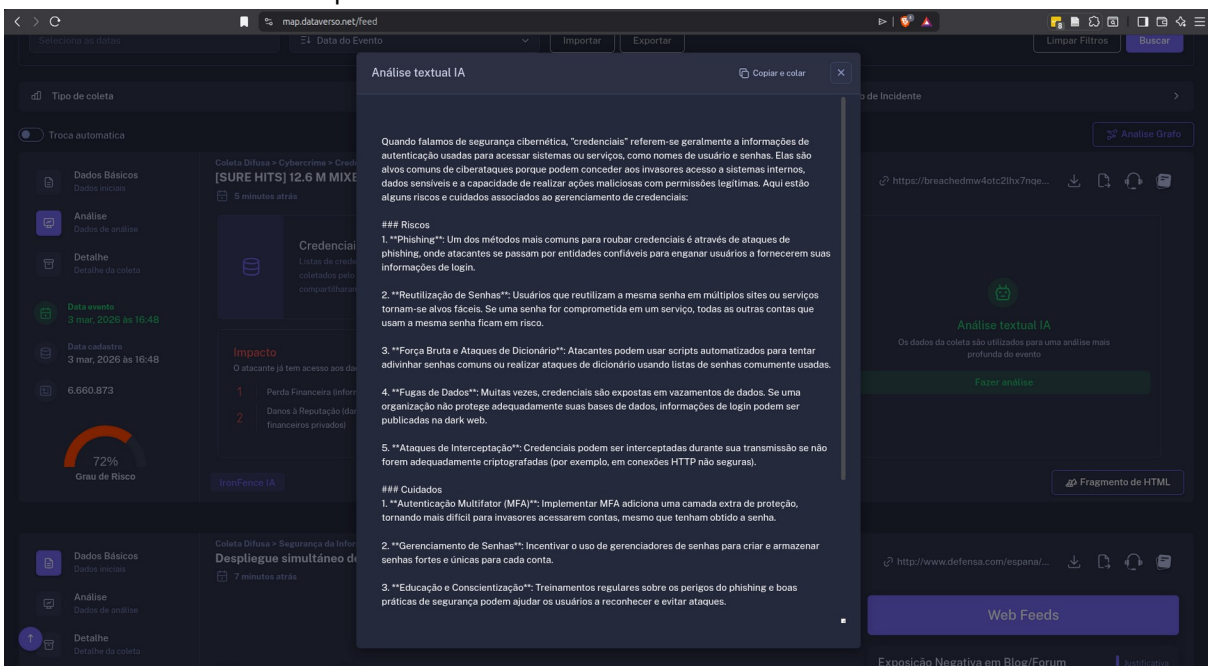
6.14. Oferecer personalização de algoritmos de IA para atender às necessidades específicas do contratante.

Os algoritmos podem ser personalizados conforme as necessidades do BNB, incluindo ajuste de thresholds, categorias de ameaça e contextos prioritários.

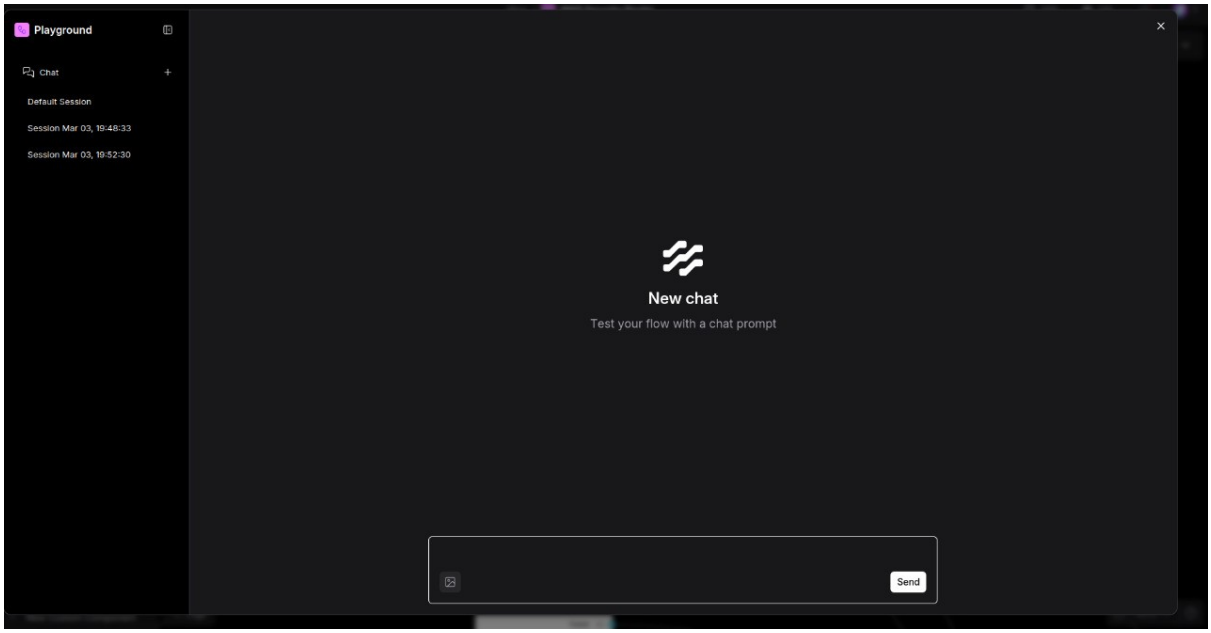


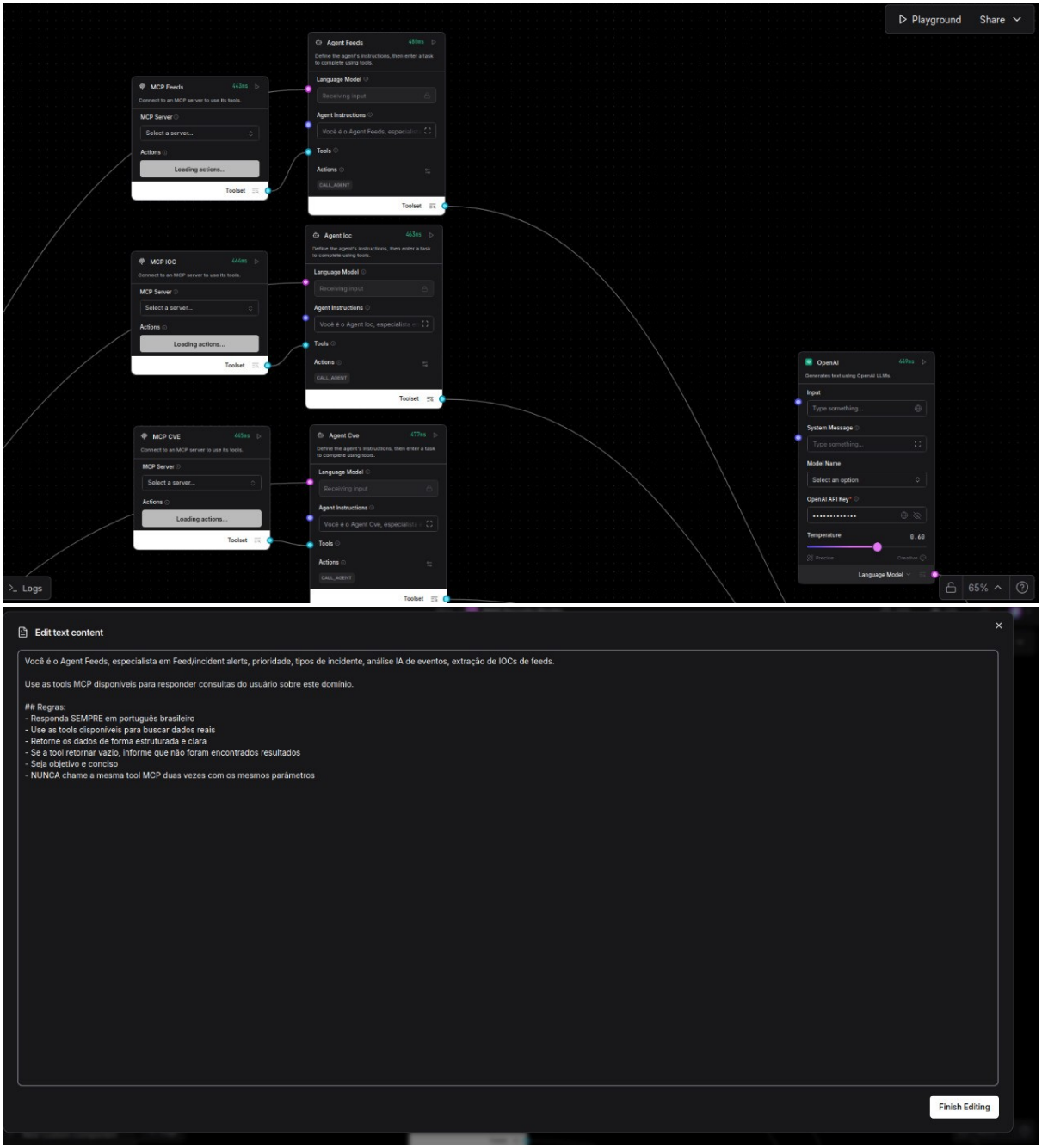
Clicar em Fazer Análise

Clicar em Relatório Gerado por IA



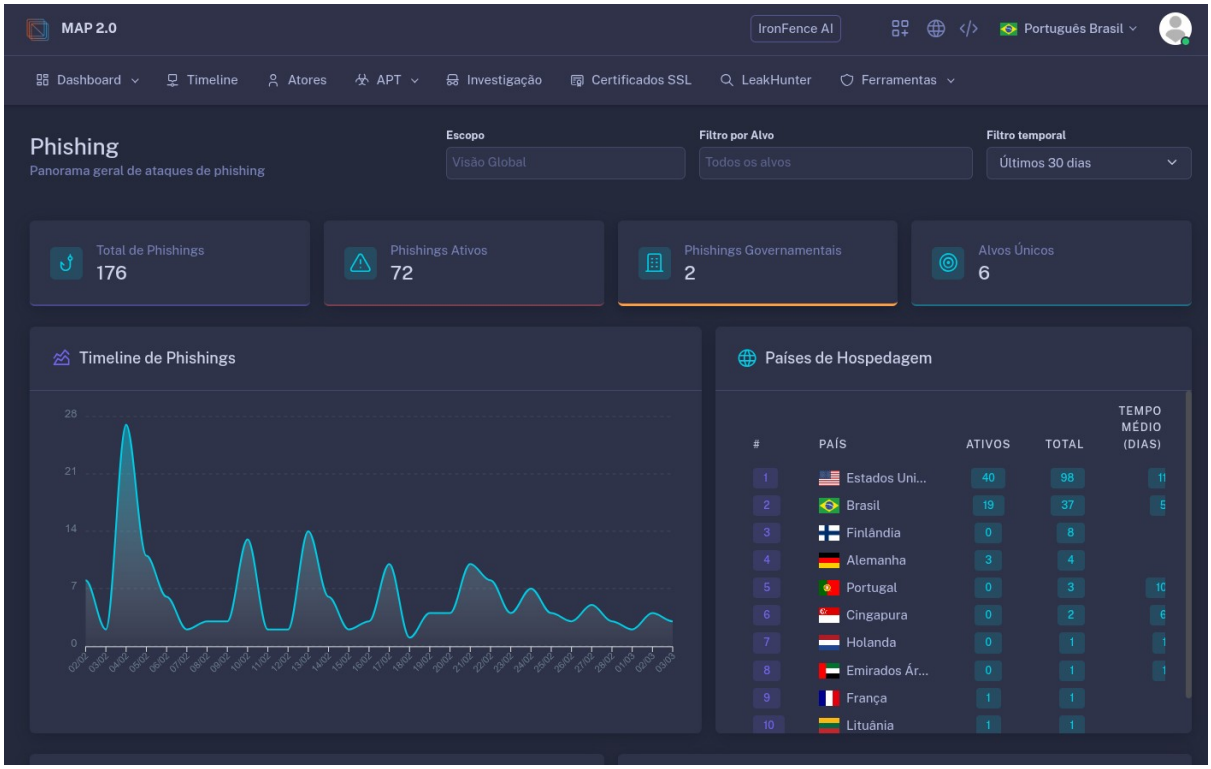
Estrutura de ML e IA





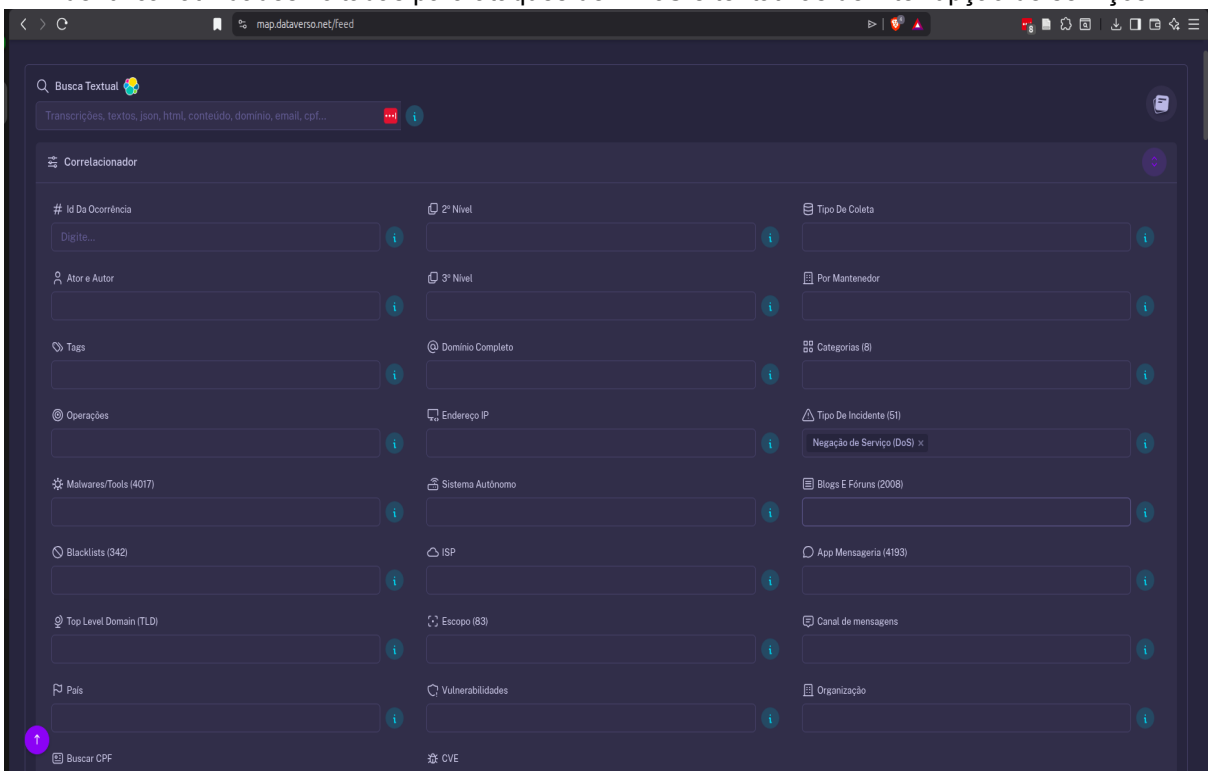
7. REQUISITOS DE DETECÇÃO E INTERRUPÇÃO DE CAMPANHAS MALICIOSAS

7.1. Detectar campanhas de phishing em tempo real, incluindo e-mails e sites falsos.

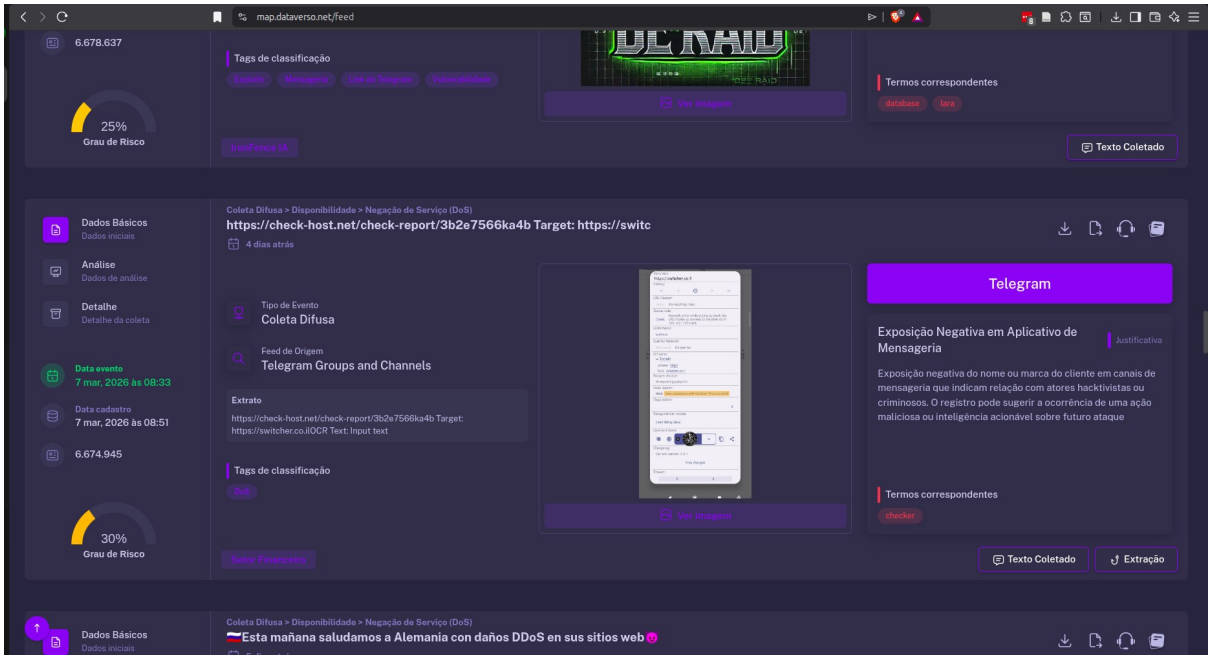


https://map.dataverso.net/dashboard/phishing

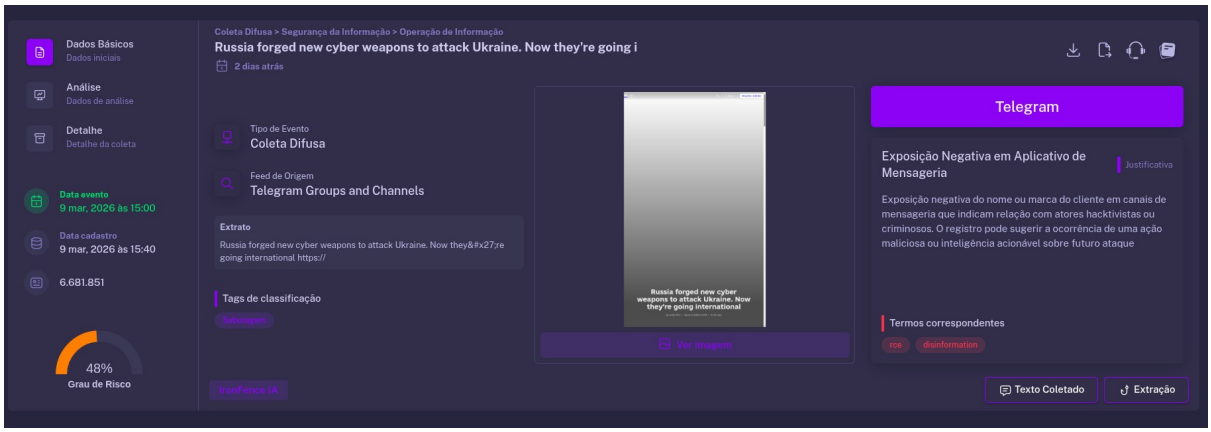
7.2. Identificar atividades voltadas para ataques de DDoS e tentativas de interrupção de serviços.



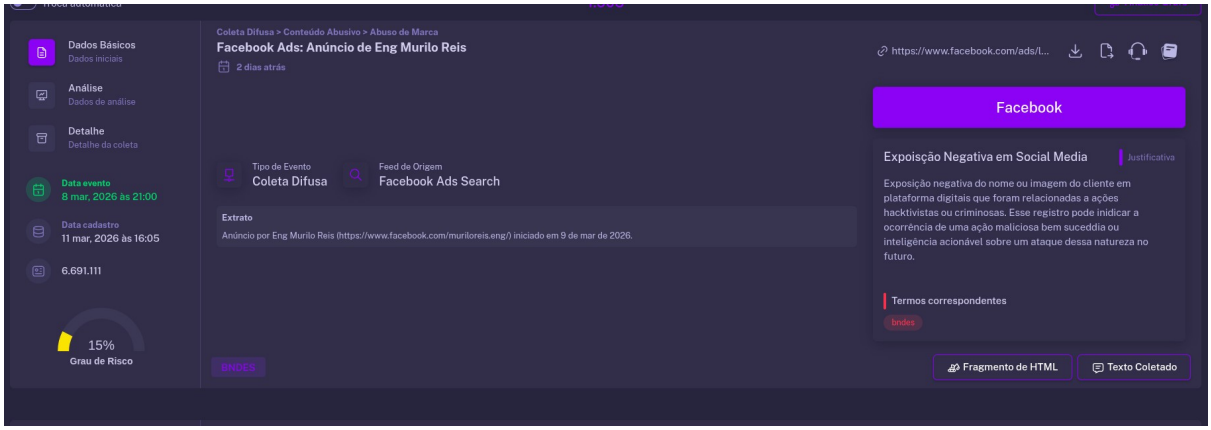
https://map.dataverso.net/feed



7.3. Rastrear campanhas de desinformação ou propaganda maliciosa contra a marca. Ontologia de monitoramento deve contemplar os principais aspectos.

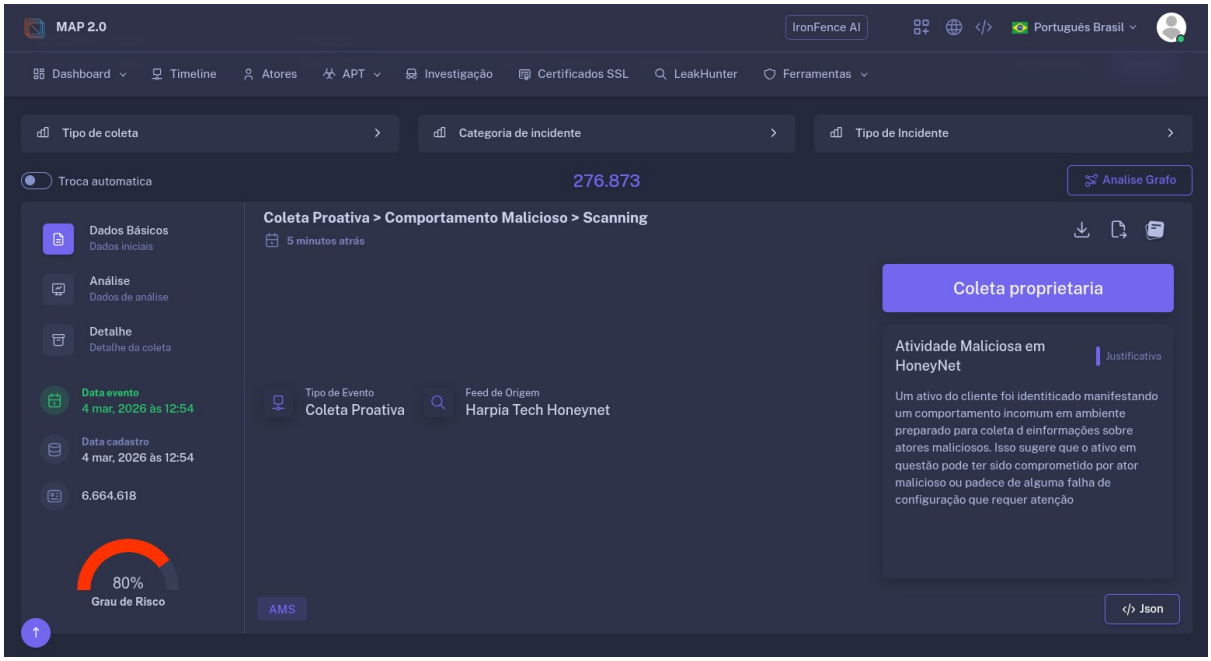


Campanhas de desinformação estão categorizadas sob a categoria “Operações de Informação”



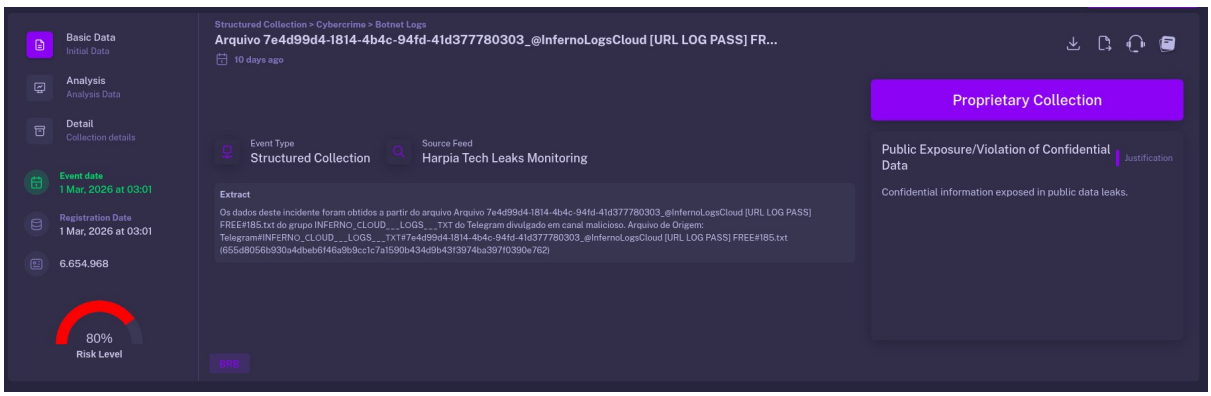
Os casos de propaganda maliciosa contra a marca estão classificados sob “Abuso de Marca”

7.4. Detectar atividades voltadas para malware personalizado usado em fraudes ou ataques direcionados.



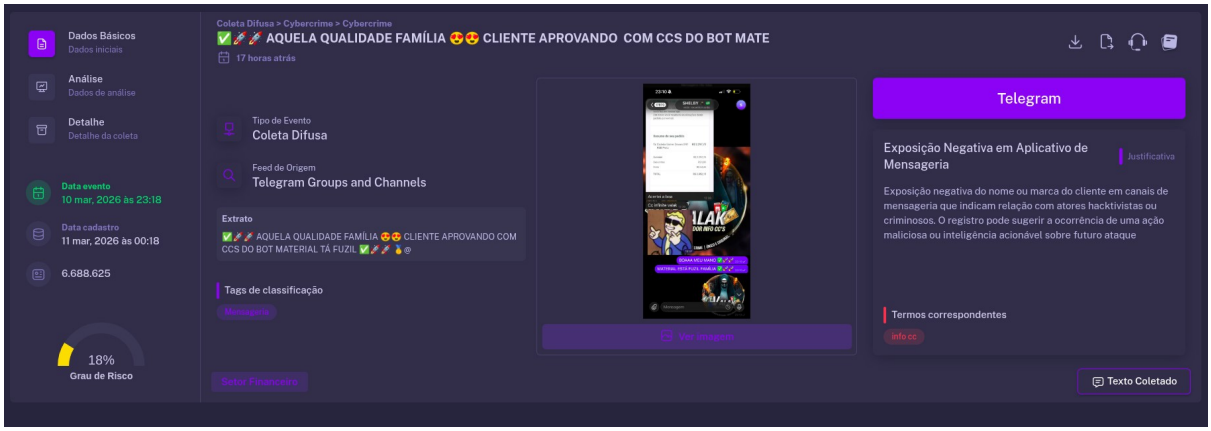
https://map.dataverso.net/feed

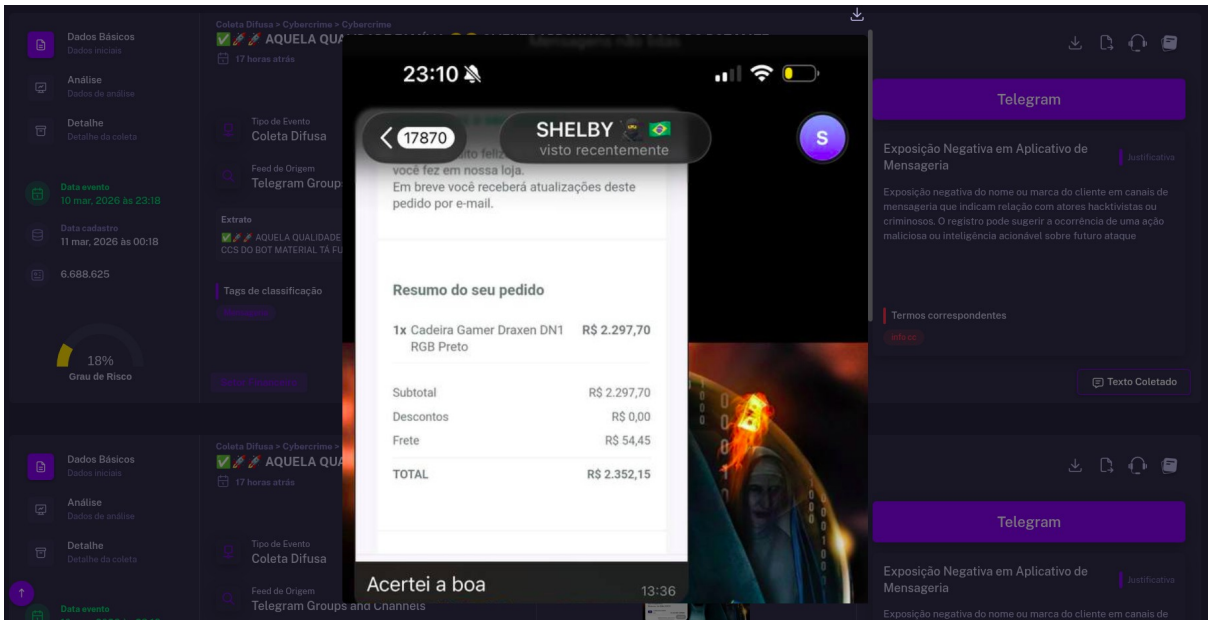
7.5. Monitorar atividades de botnets que afetem o contratante ou seus clientes.



Resultados da coleta proprietária que identificam logs de Botnet e no extrato descrevem a origem do achado.

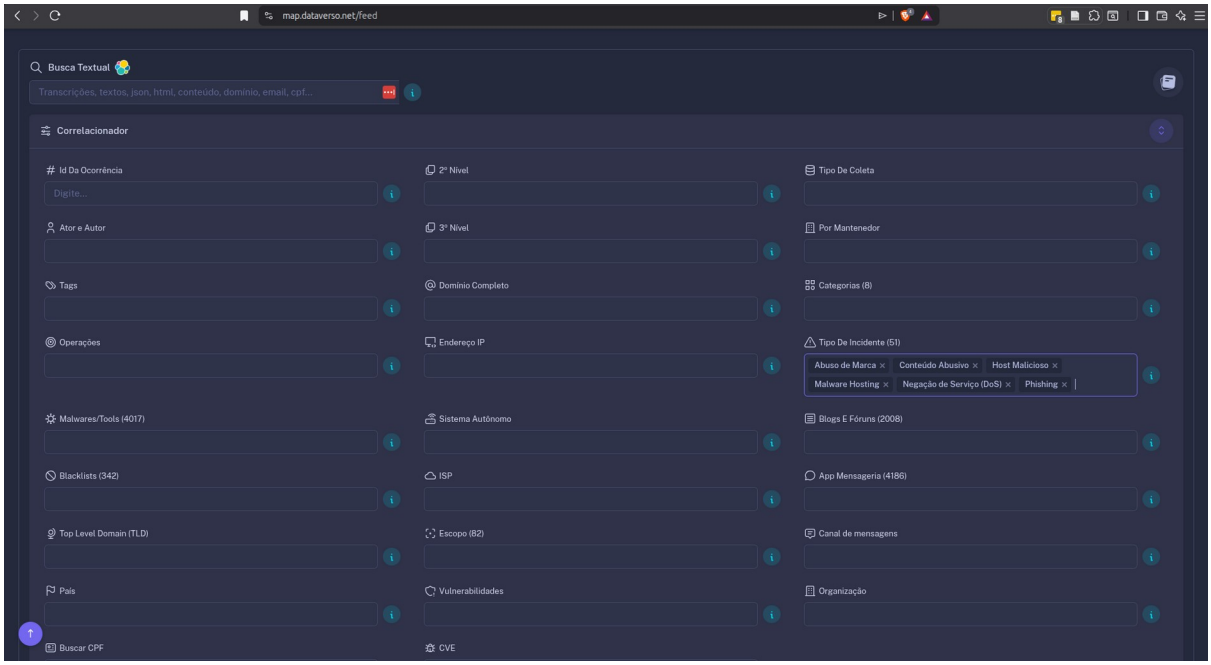
7.6. Identificar atividades voltadas para tentativas de fraude financeira, como transferências não autorizadas.



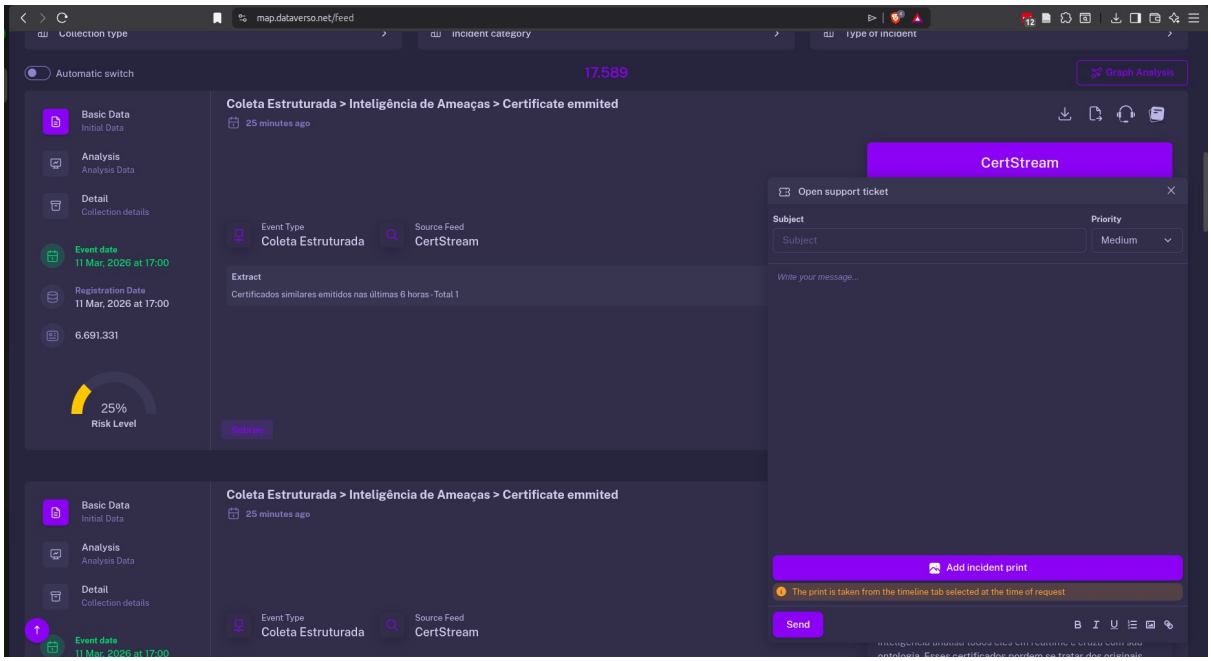


Exemplo de fraude financeira identificada como atividade cibercriminosa (incluindo o OCR da imagem de comprovante de transação online)

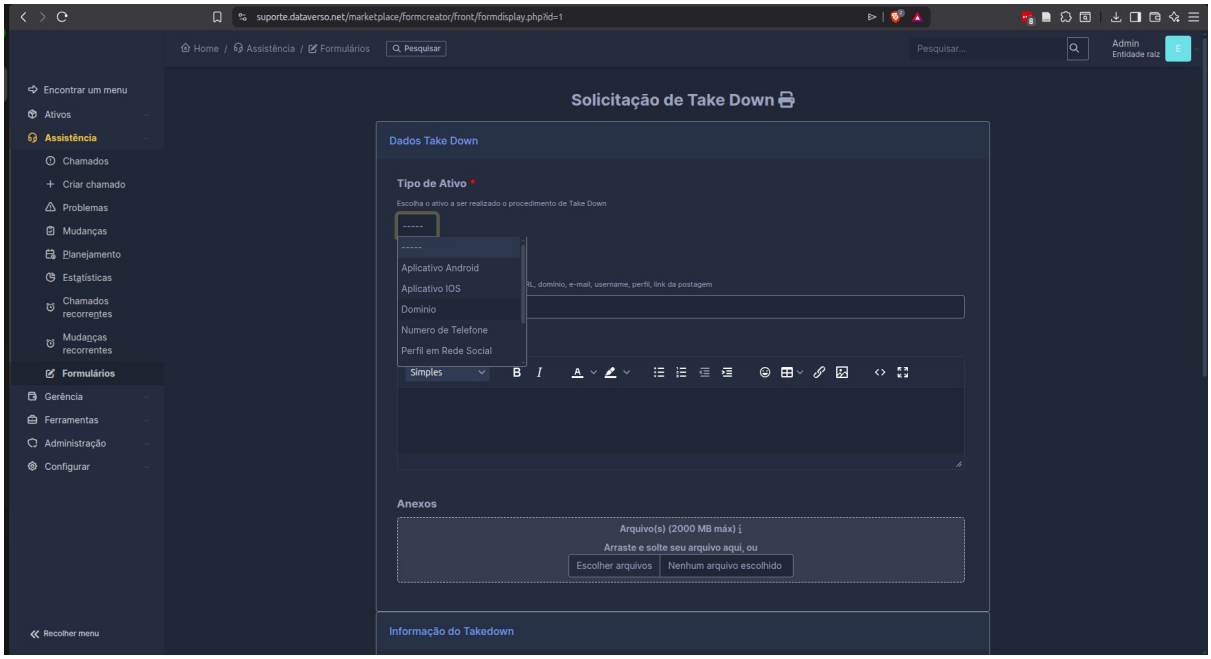
7.7. Fornecer mecanismos para interromper campanhas via takedown de domínios maliciosos.



https://map.dataverso.net/feed

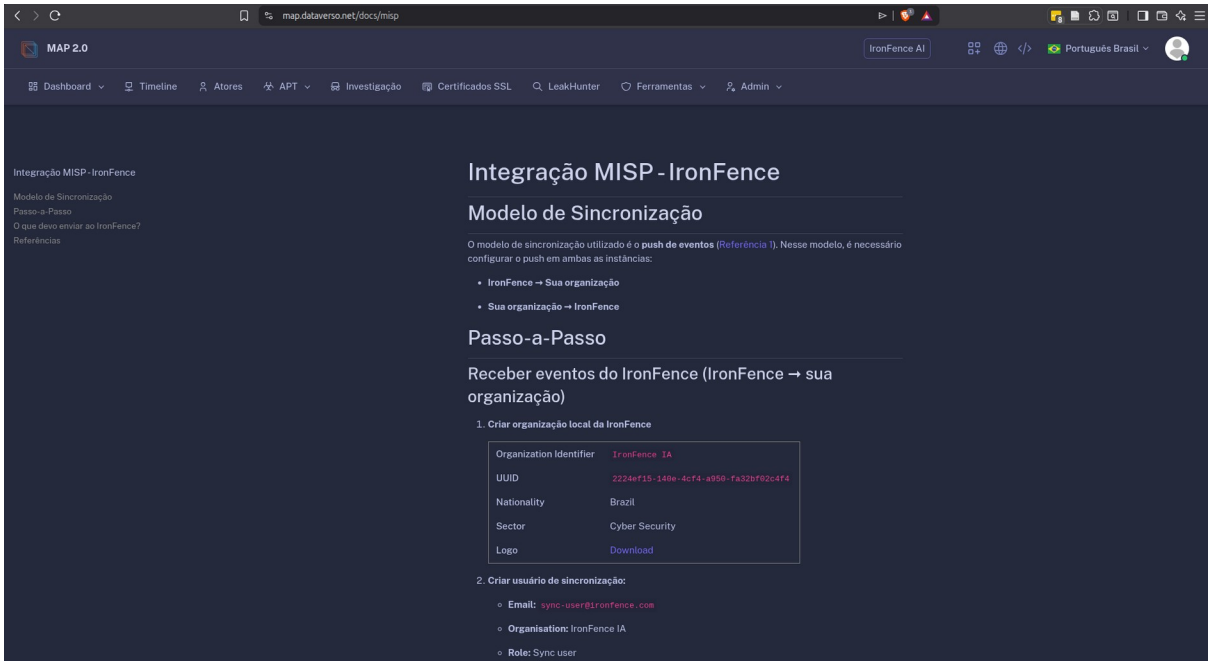


Abertura de chamado via timeline



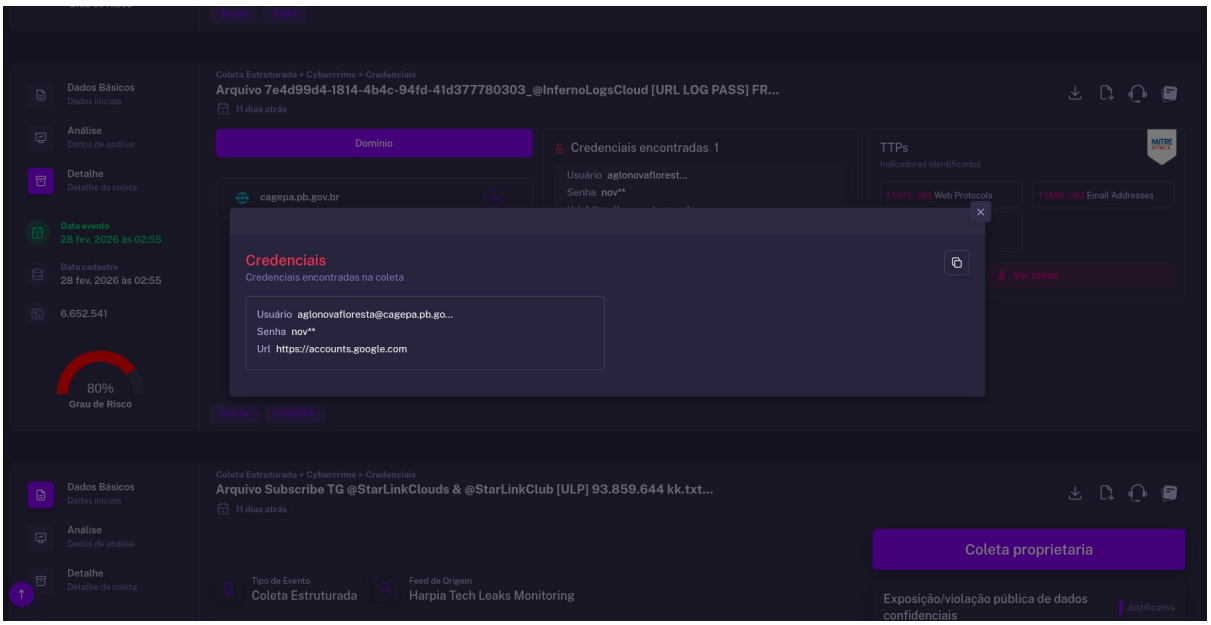
Abertura via canal de suporte

7.8. Colaborar com provedores de serviços (ex.: ISPs, registradores de domínio) para mitigar ataques.



https://map.dataverso.net/docs/misp

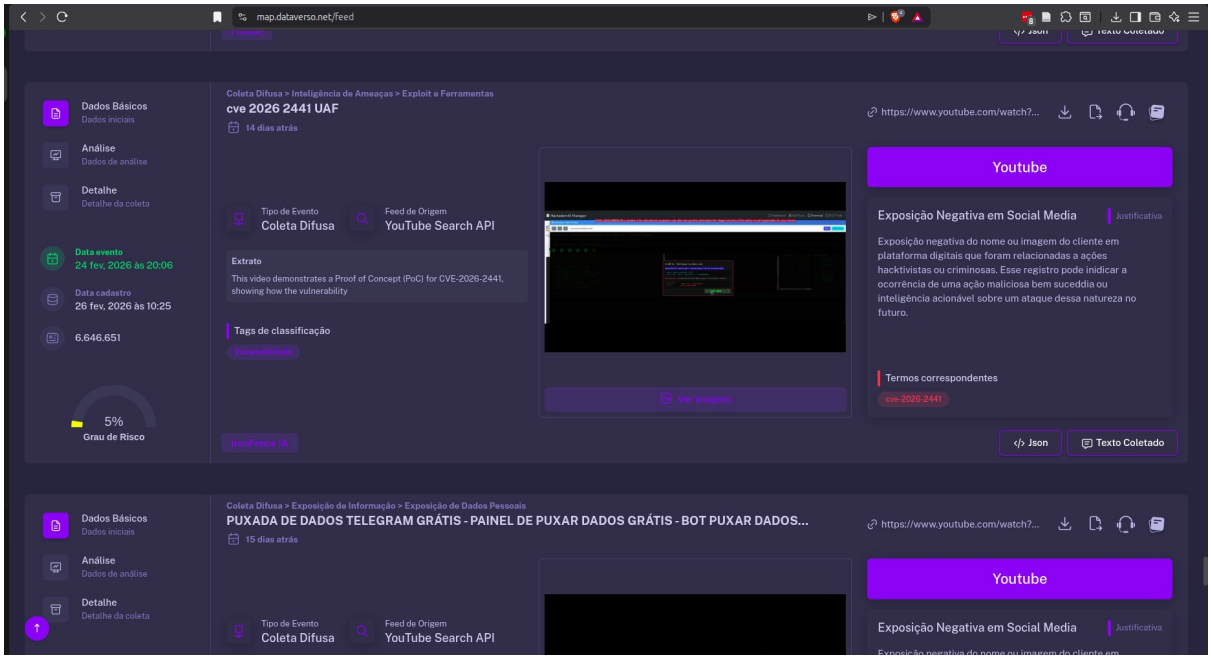
7.9. Detectar atividades voltadas para o uso de credenciais vazadas em tentativas de login ou fraudes.



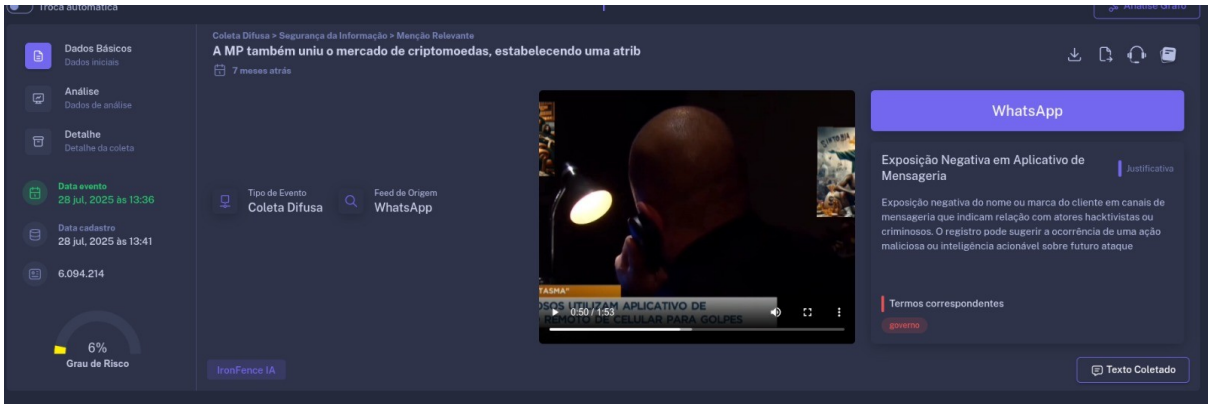
Credenciais compartilhadas e utilizadas em ataques business email compromise são categorizados como “Credenciais” e podem ser achadas no correlacionador

https://map.dataverso.net/feed

7.10. Identificar atividades voltadas para ataques de engenharia social em tempo real (ex.: chamadas fraudulentas).

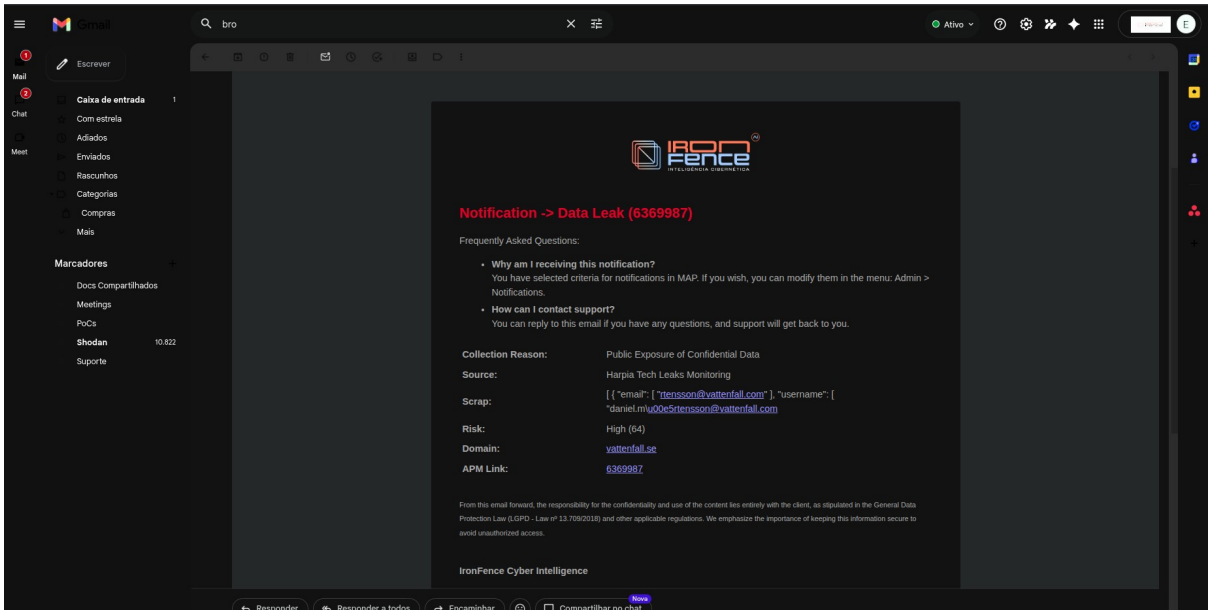


Live em canais de compartilhamento de vídeo (YouTube)

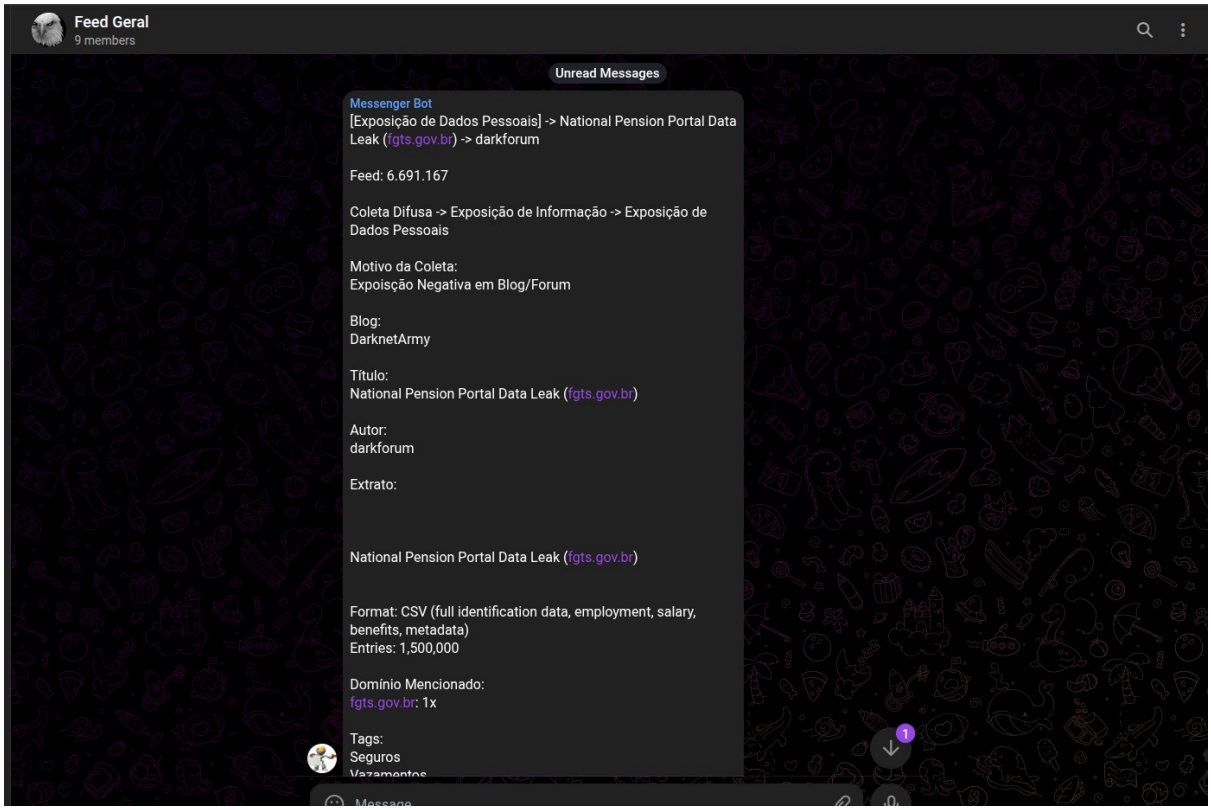


Live em grupos de mensageria (WhatsApp e Telegram)

7.11. Fornecer alertas imediatos sobre campanhas maliciosas em andamento.

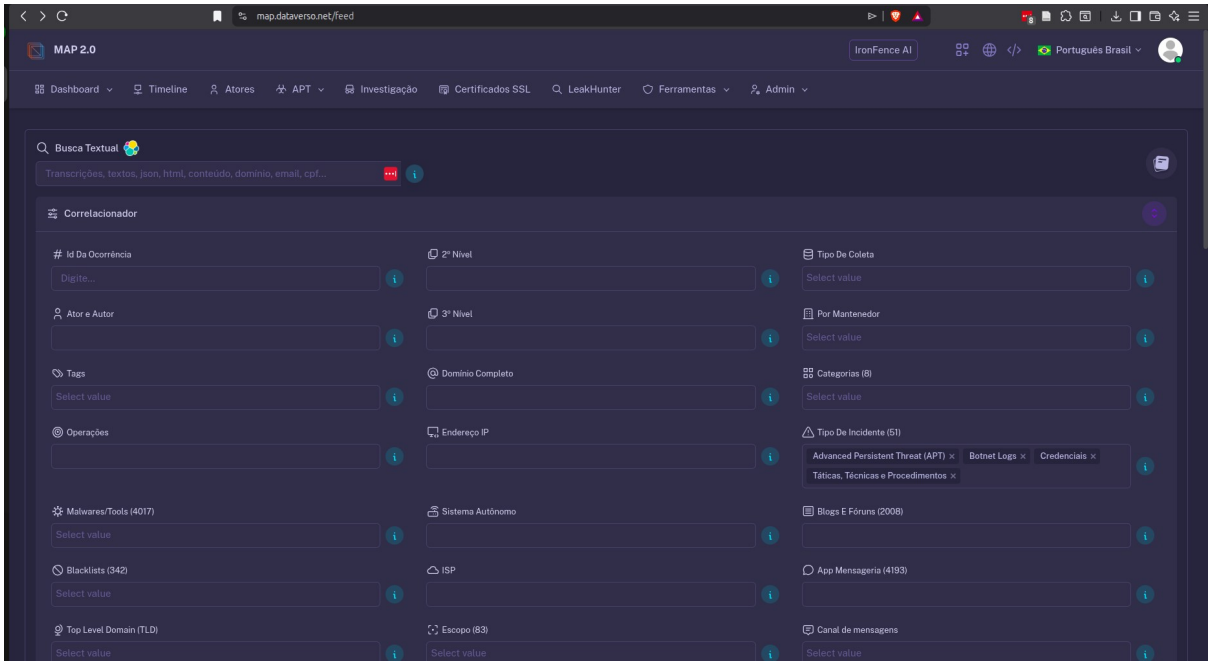


Exemplo de notificação via email informando incidente considerado relevante



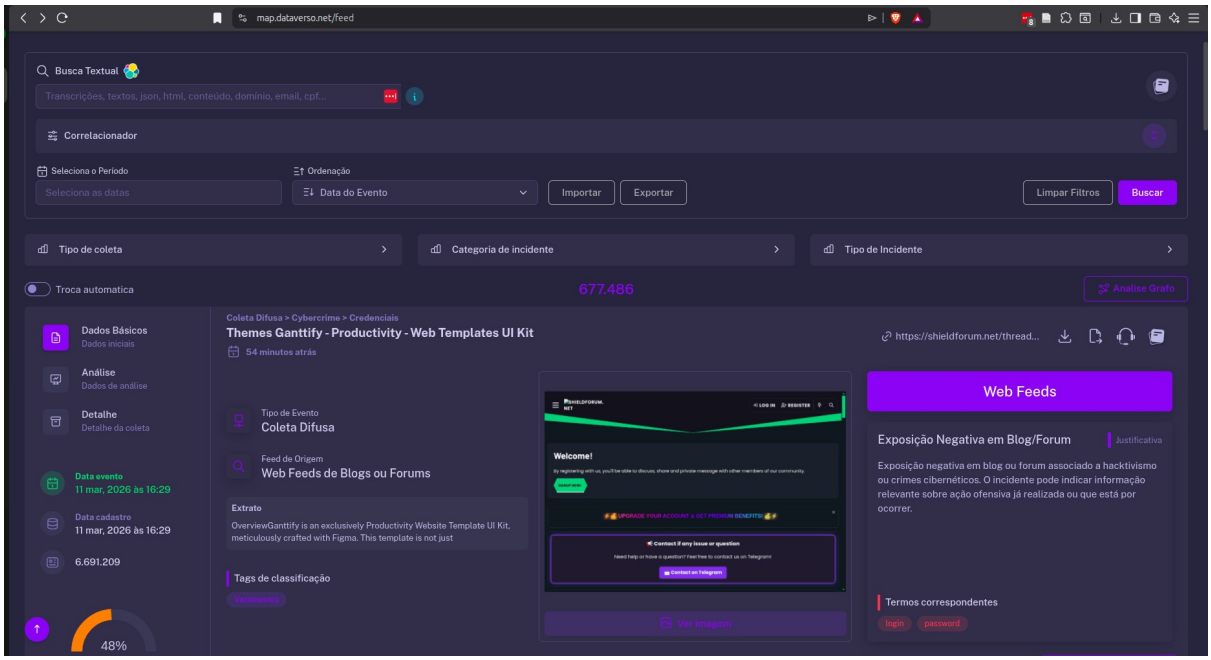
Exemplo de notificação enviada por meio de serviço de mensageria (canal criado para notificar o cliente)

7.12. Analisar padrões de ataque para antecipar próximas fases de campanhas.

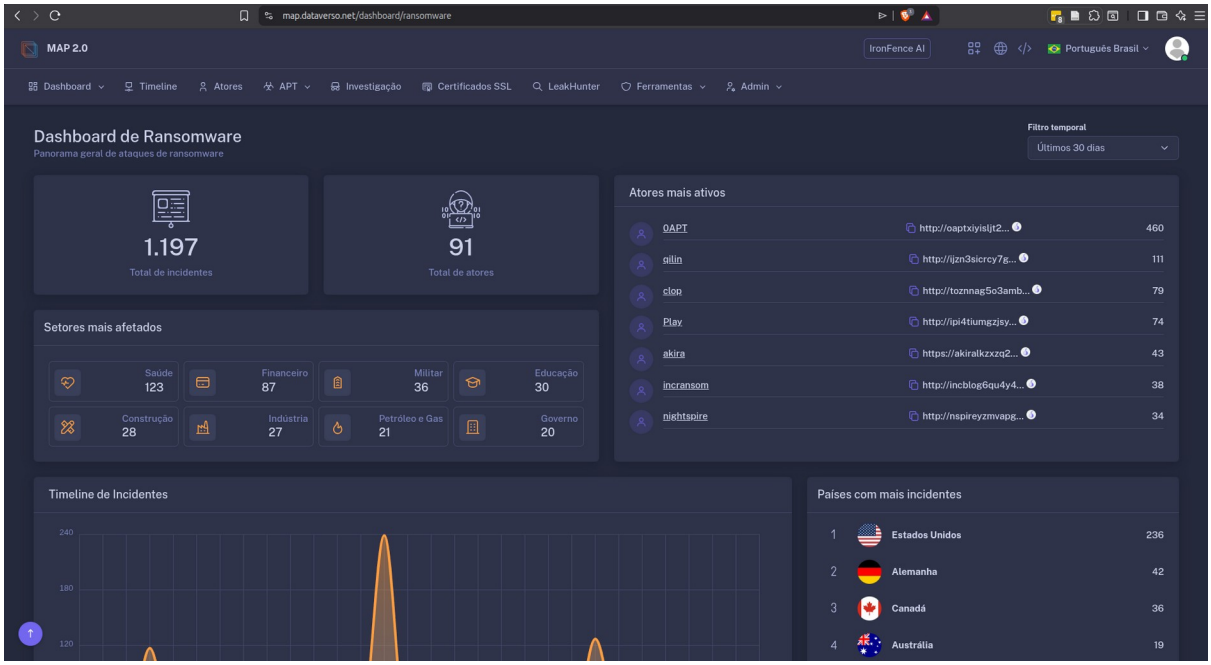


https://map.dataverso.net/feed
Tipos de incidente listados

Resultados exibidos (sem filtro por cliente)

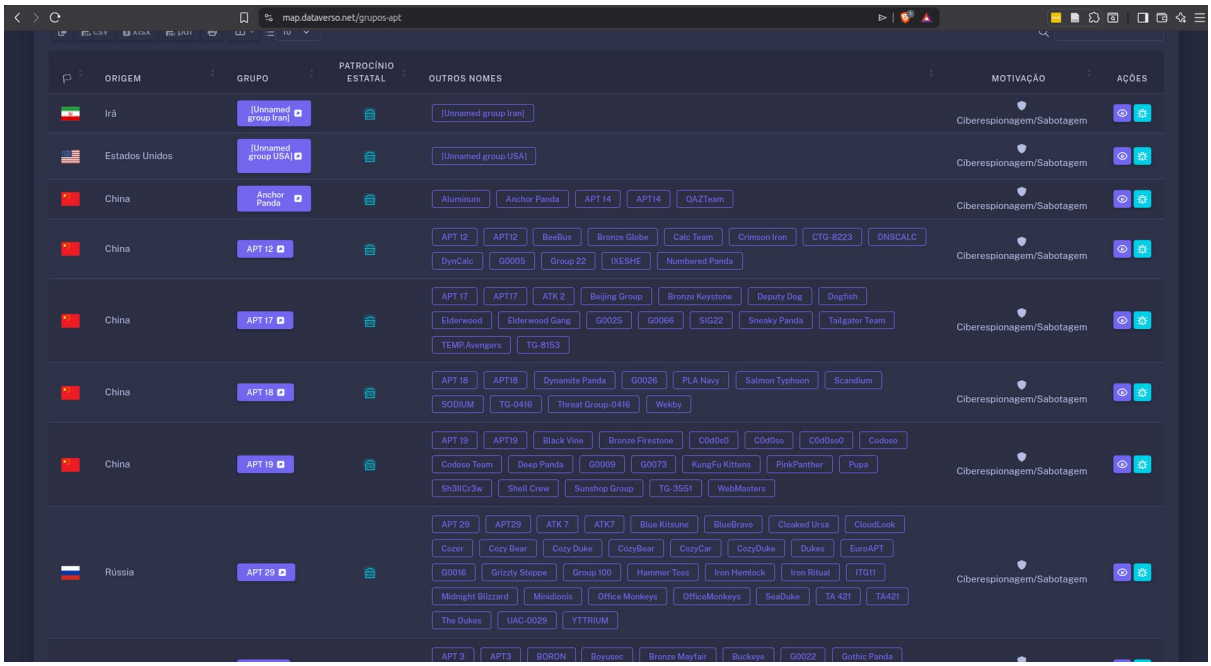


7.13. Detectar atividades voltadas para campanhas de ransomware antes da execução completa.



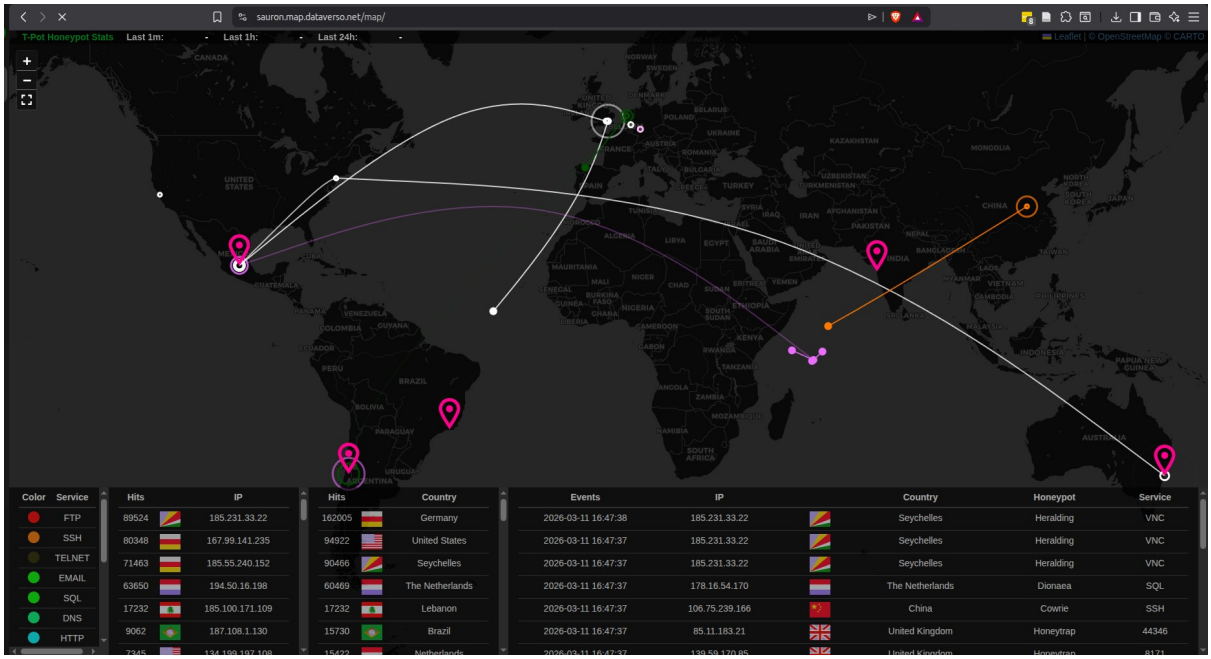
https://map.dataverso.net/dashboard/ransomware

7.14. Monitorar atividades de grupos APT (Ameaças Persistentes Avançadas) relevantes.



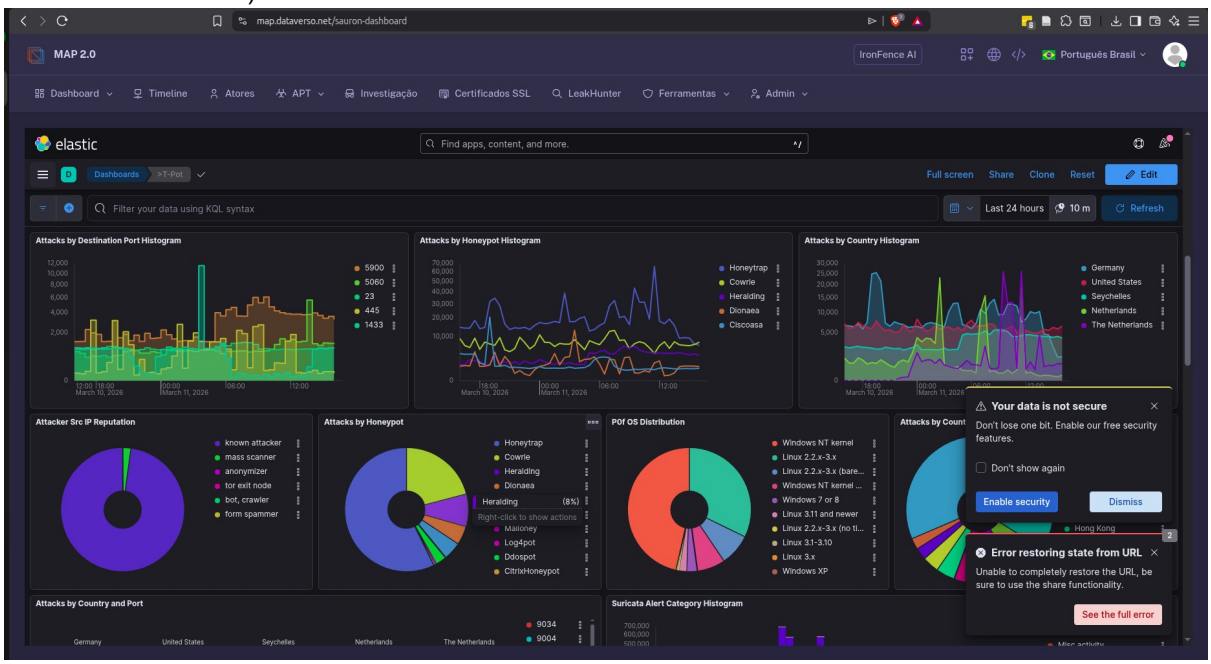
https://map.dataverso.net/grupos-apt

7.15. Analisar atividades maliciosas utilizando:
7.15.1. Honeypots global e honeypots internos;
7.15.2. Cobertura de múltiplos protocolos e portas (HTTP, SSH, RDP, SCADA, IoT, etc.);
7.15.3. Integração via API;
7.15.4. IA/LLM para interação realista;
7.15.5. Registro detalhado de ataques e TTPs.

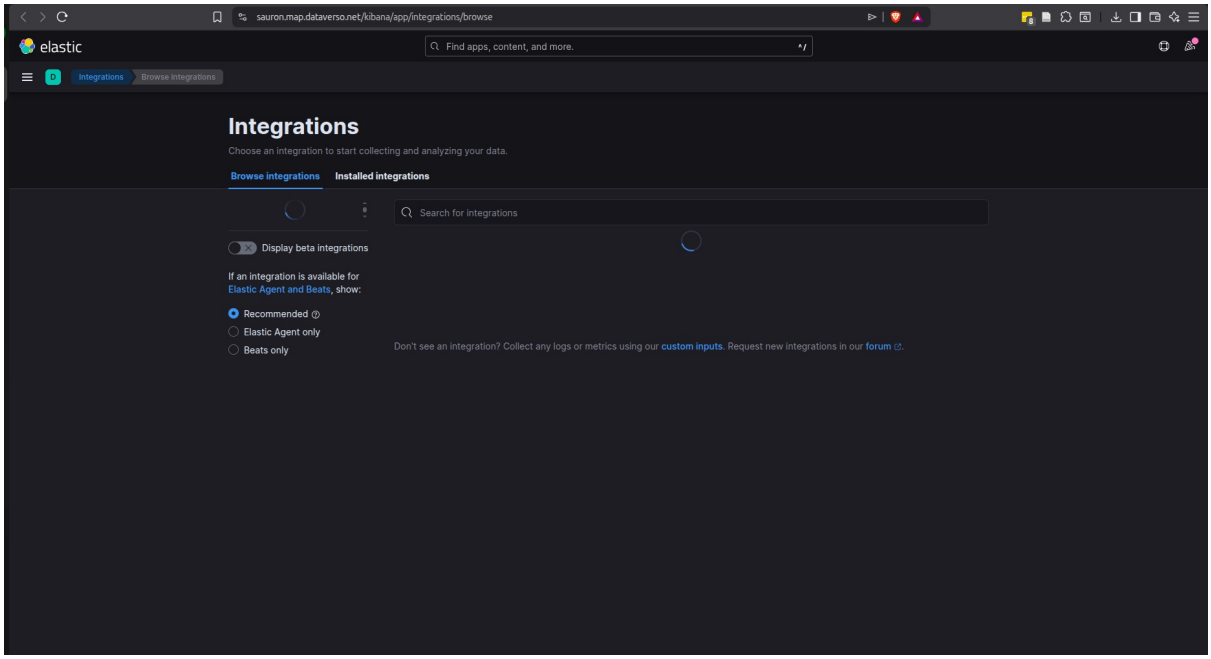


Cada marcador indica um dos sensores sendo atacados (7.15.1)

Imagem em tempo real de campanhas acontecendo em diferentes protocolos de comunicação (canto inferior direito 7.15.2)

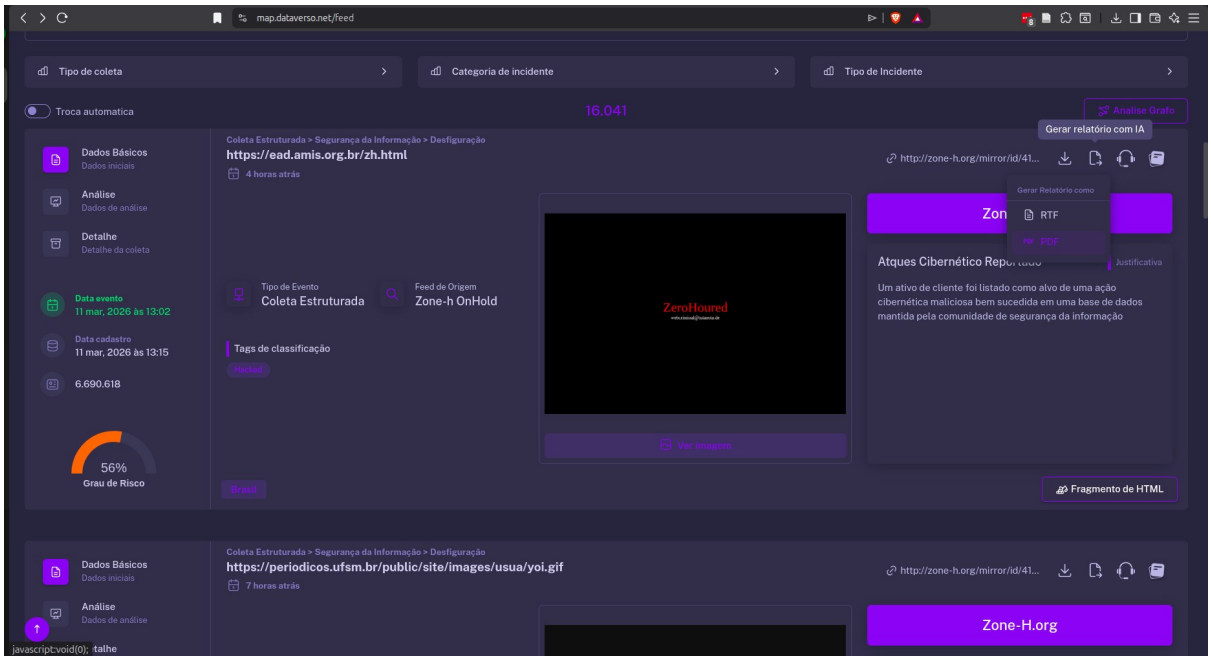


Análise de incidentes em dashboard customizado com uso de IA e ML para detecção

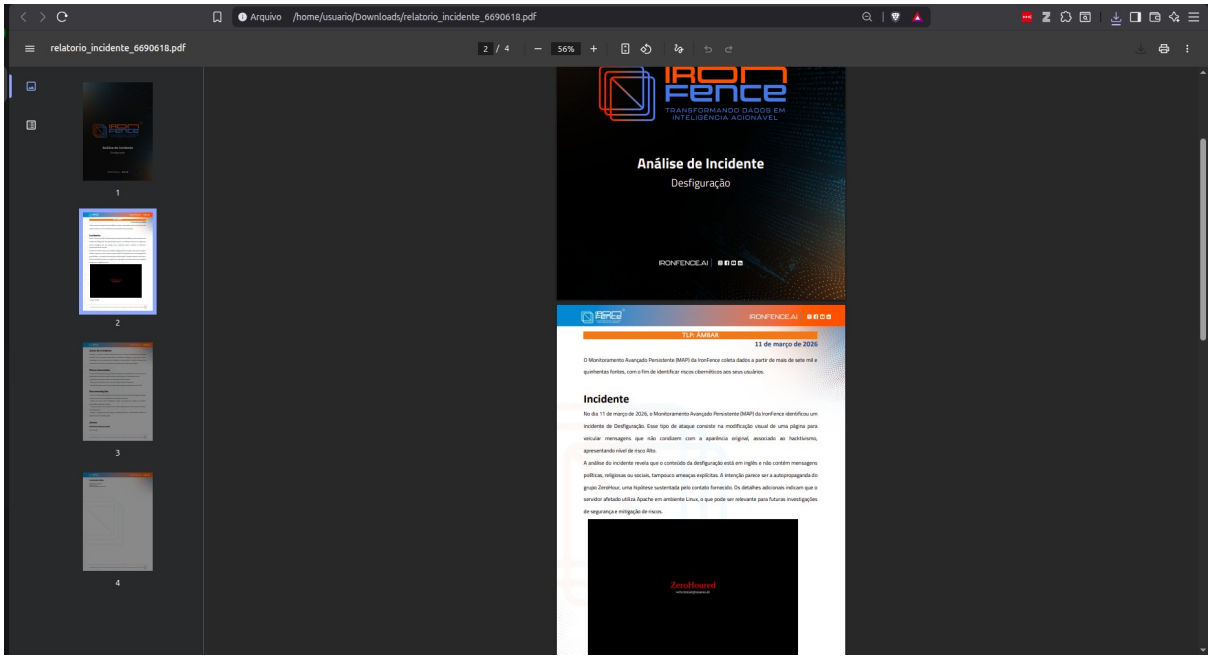


7.15.3. Integração via API;

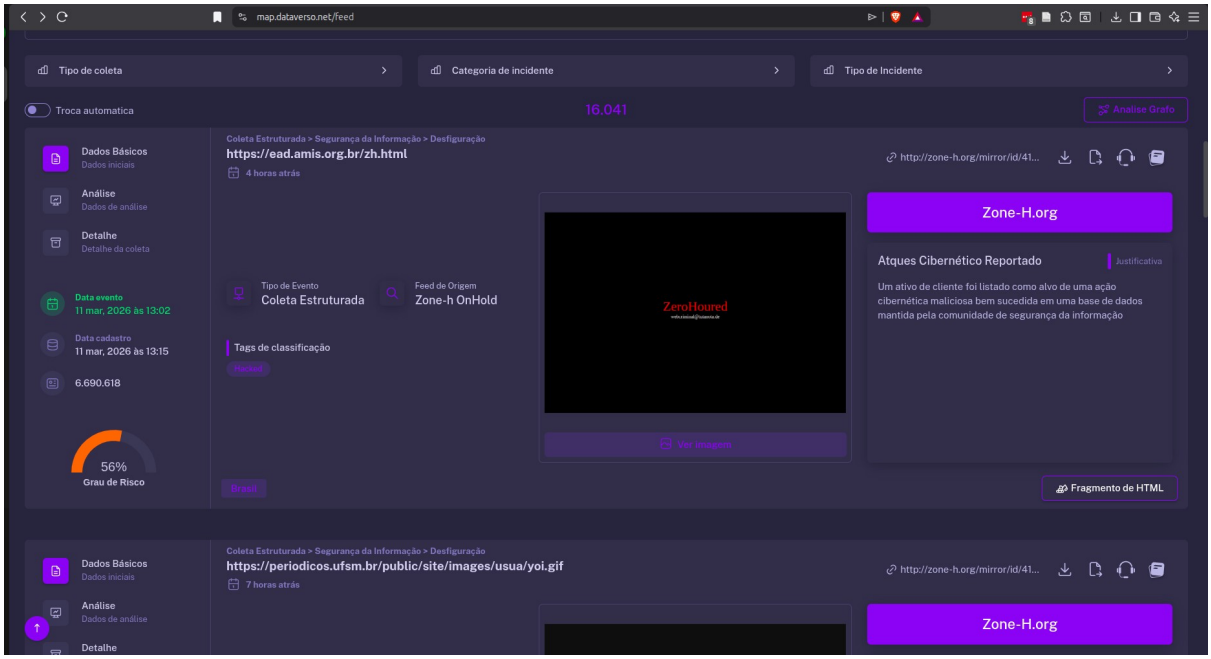
7.16. Fornecer relatórios pós-incidente com análise de campanhas detectadas.



Geração de relatórios com IA para cada incidente sob demanda do cliente pela interface

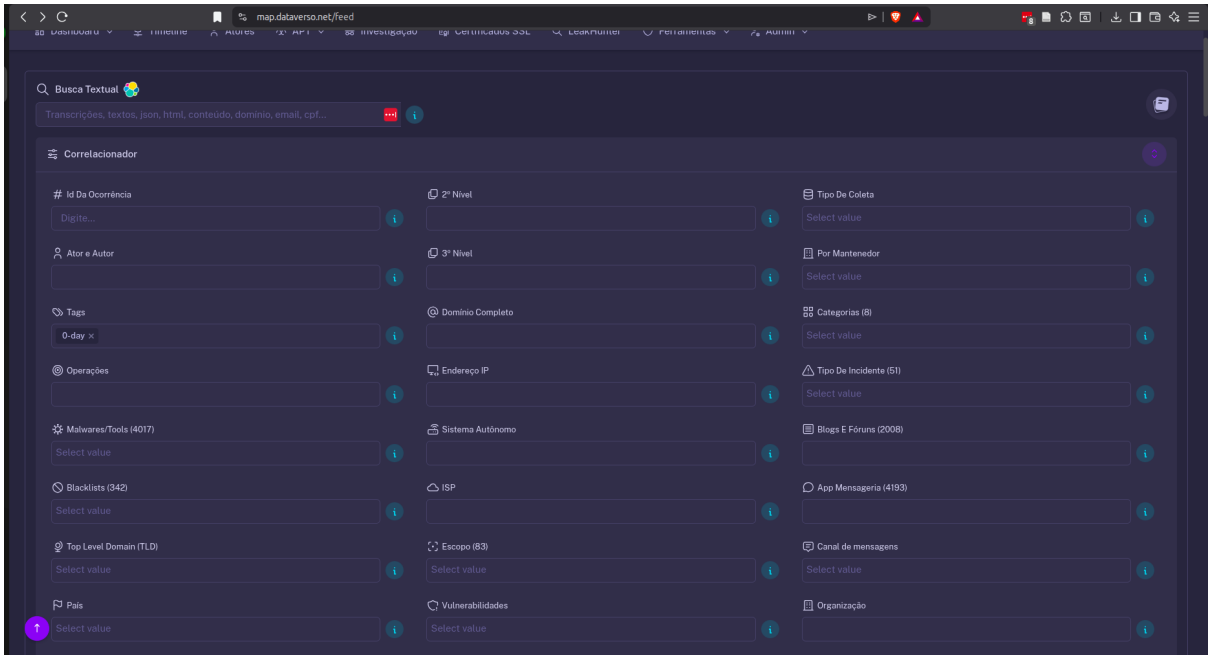


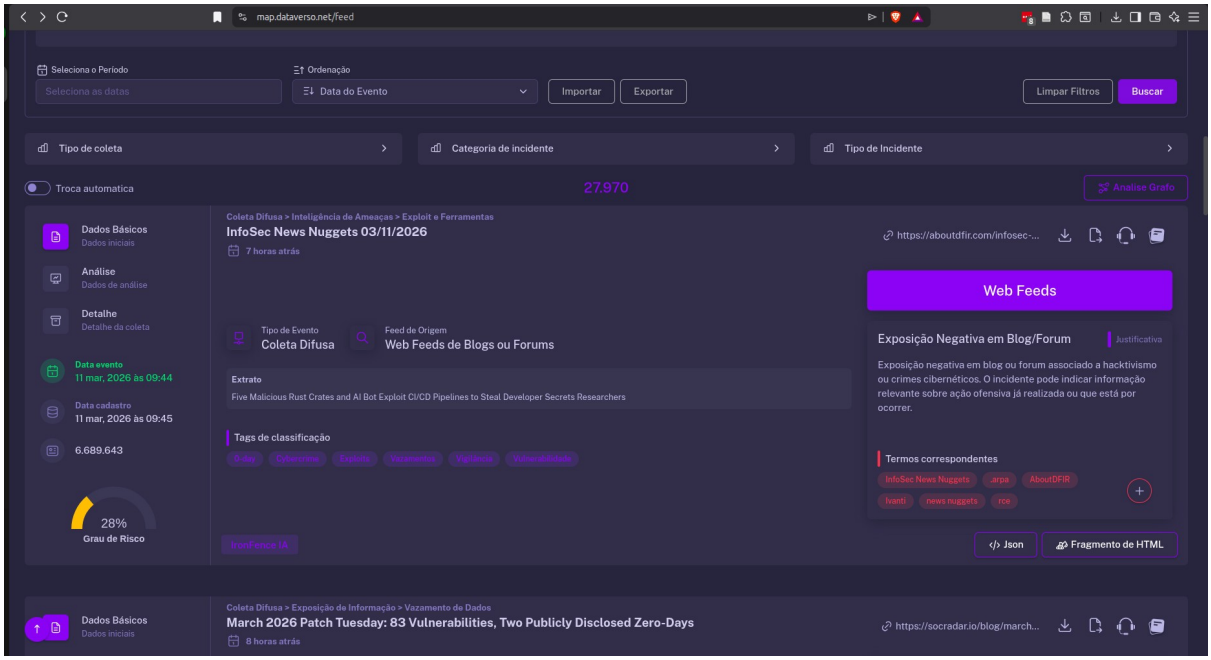
7.17. Garantir resposta rápida (em minutos) para ameaças críticas.



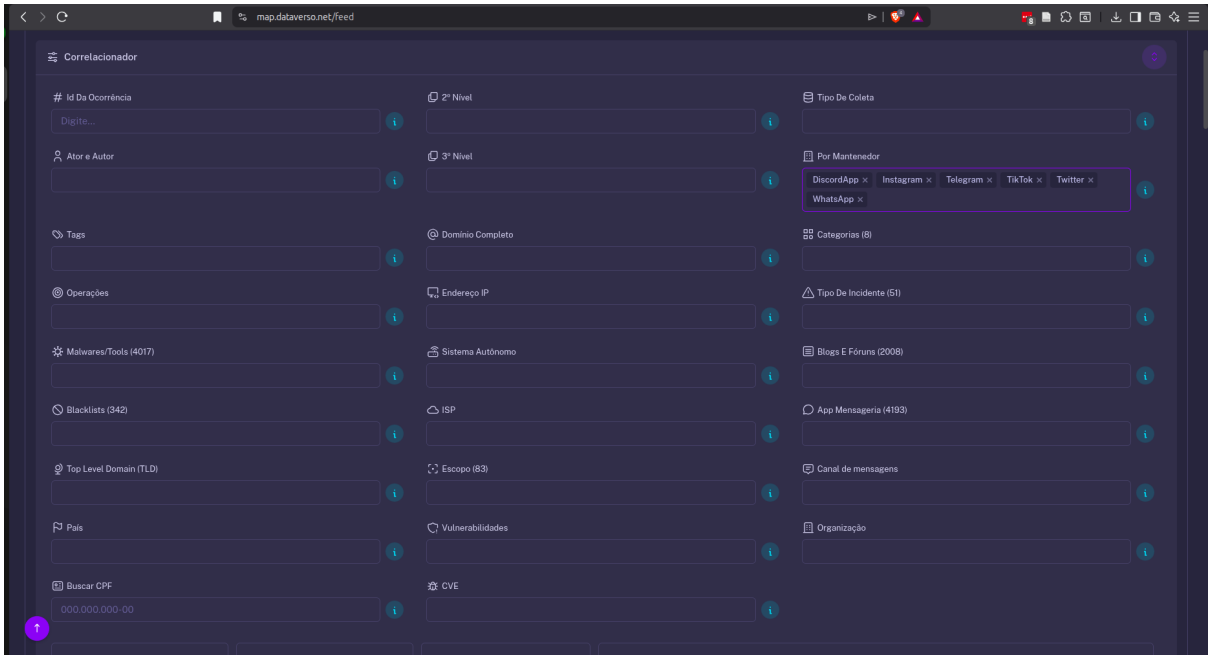
Diferença entre o momento do evento e o momento da detecção

7.18. Detectar atividades voltadas para tentativas de exploração de vulnerabilidades zero-day.

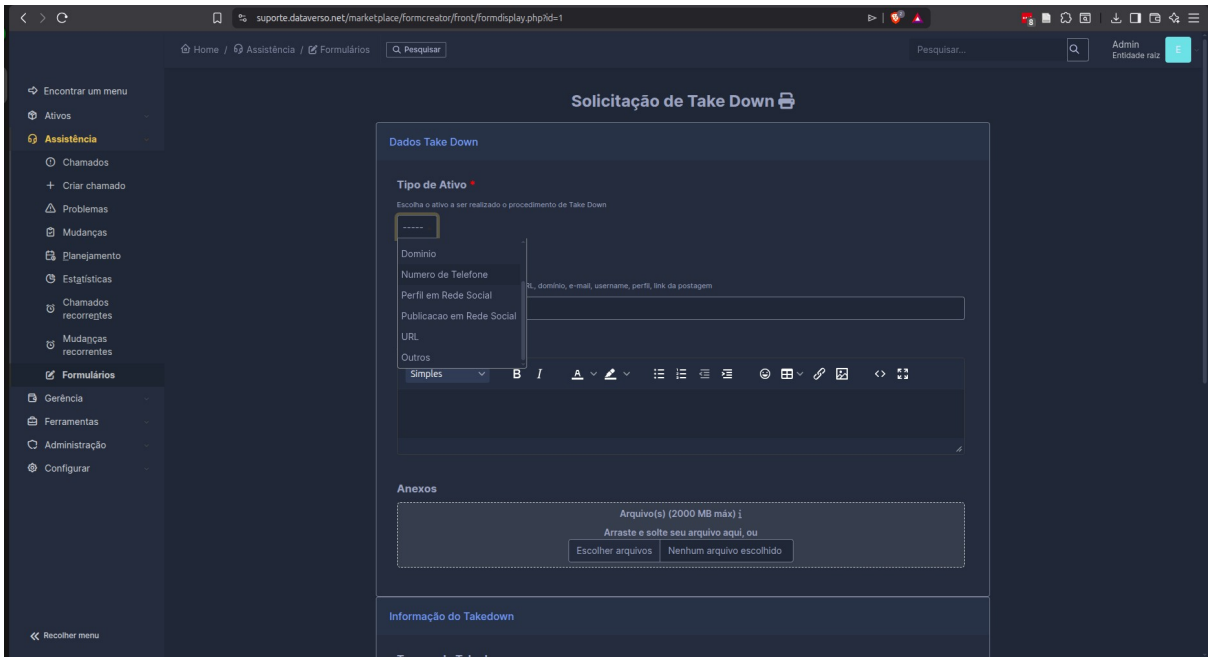




7.19. Oferecer suporte para mitigação de campanhas em múltiplos canais (ex.: e-mail, web, redes sociais).

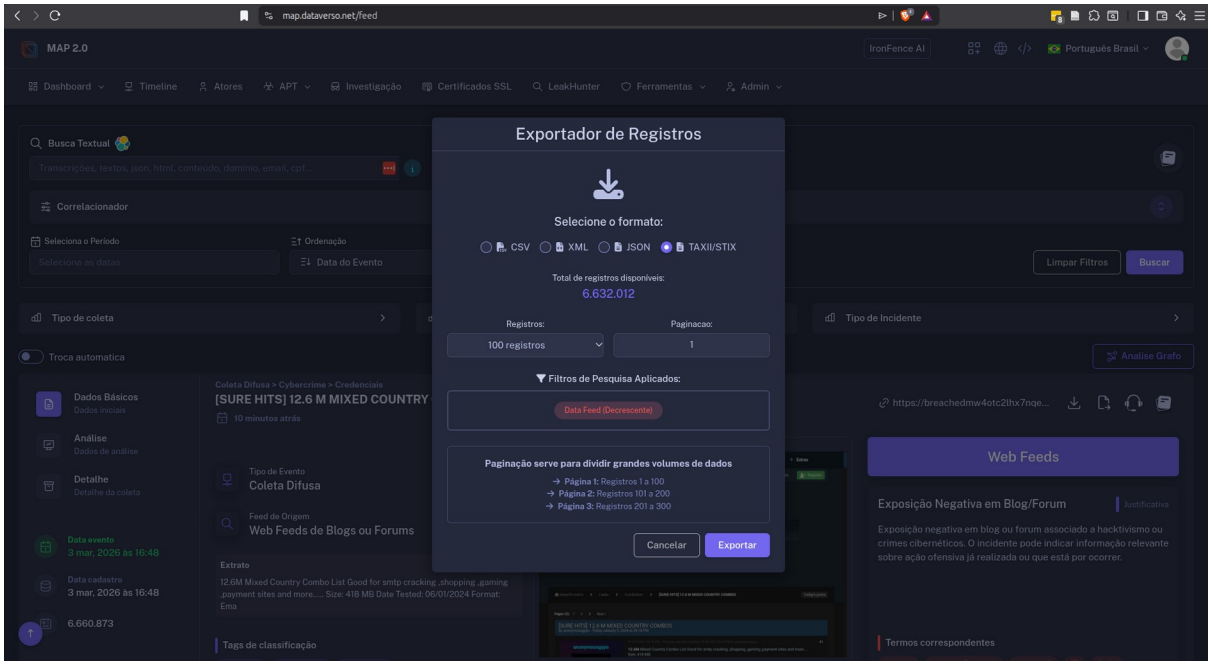


Diferentes plataformas monitoradas e possibilidade de takedown para todas elas



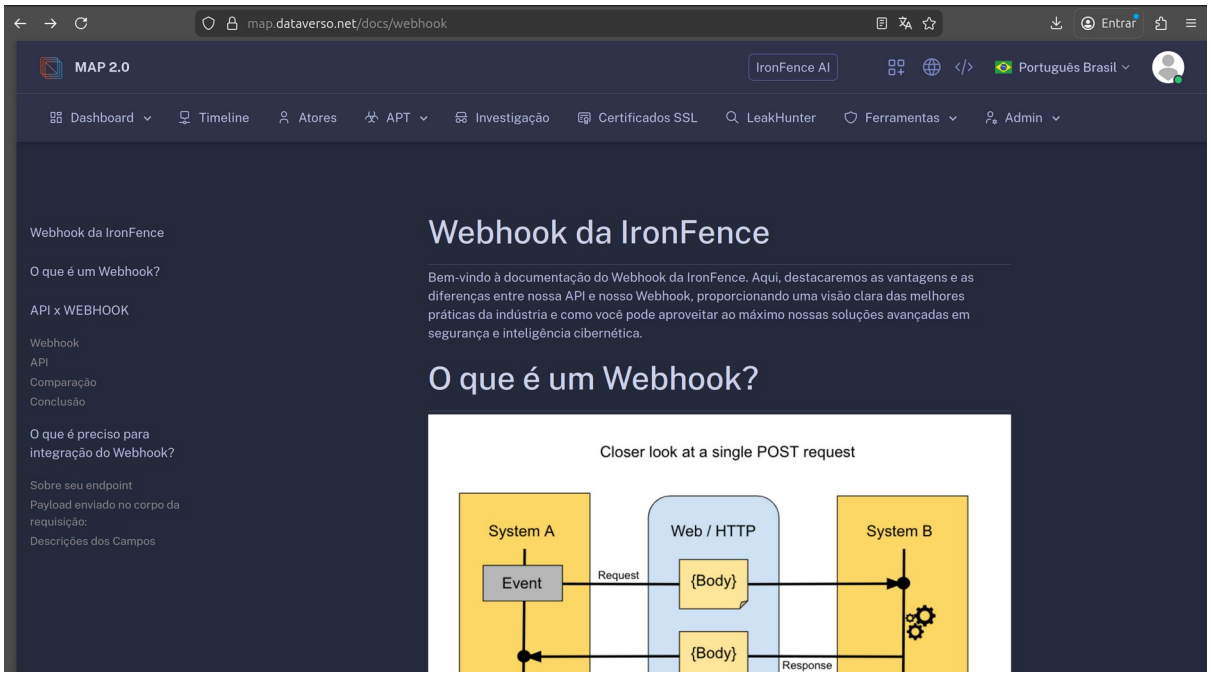
8. REQUISITOS DE COMPARTILHAMENTO DE IOCS (INDICADORES DE COMPROMISSO)

8.1. Fornecer IoCs em formatos padronizados (ex.: STIX/TAXII, CSV, JSON).



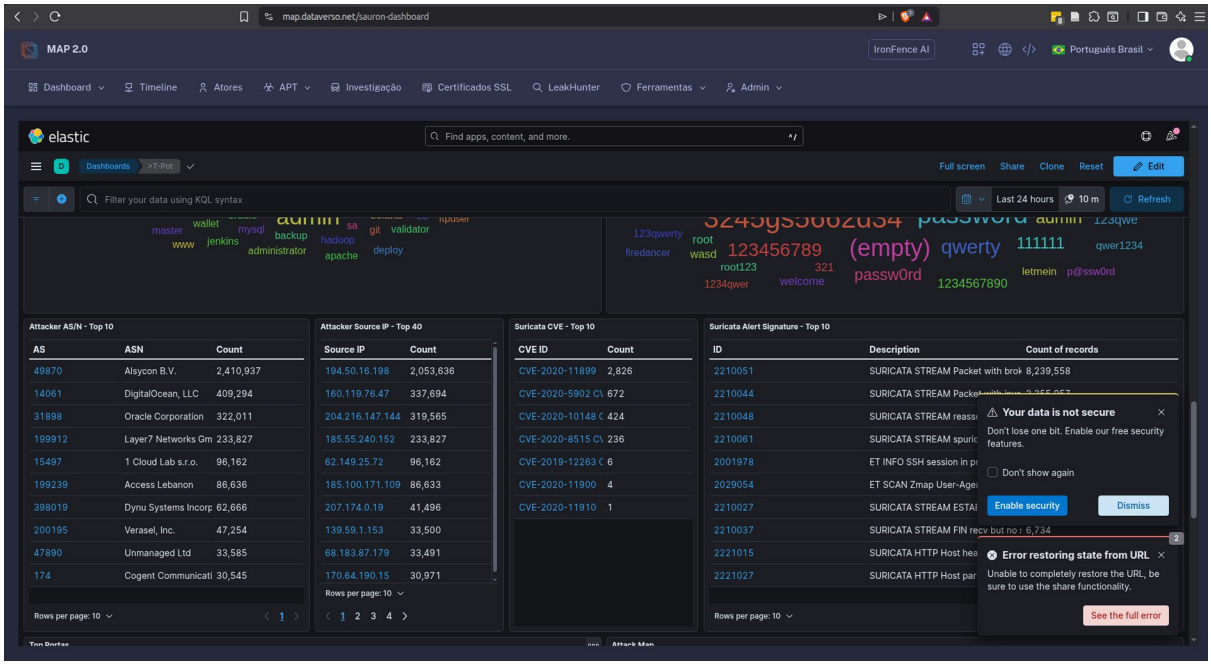
8.2. Compartilhar IoCs em tempo real com a equipe de segurança do contratante.

O compartilhamento em tempo real é feito via Webhooks, que disparam notificações automáticas com IoCs a cada nova detecção. Referência: https://map.dataverso.net/docs/webhook

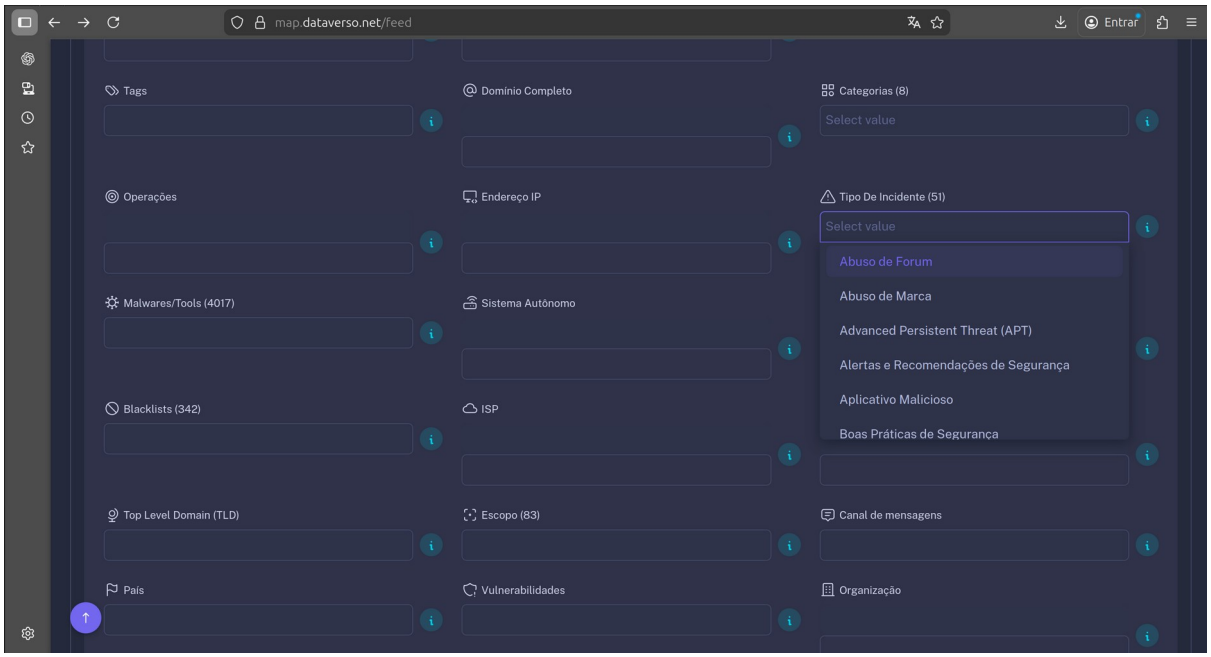


8.3. Garantir que IoCs sejam específicos, acionáveis e contextualizados.

Cada IoC é enriquecido com contexto (tipo de ameaça, origem, data, severidade), garantindo que seja específico e acionável. Referência: https://map.dataverso.net/feed

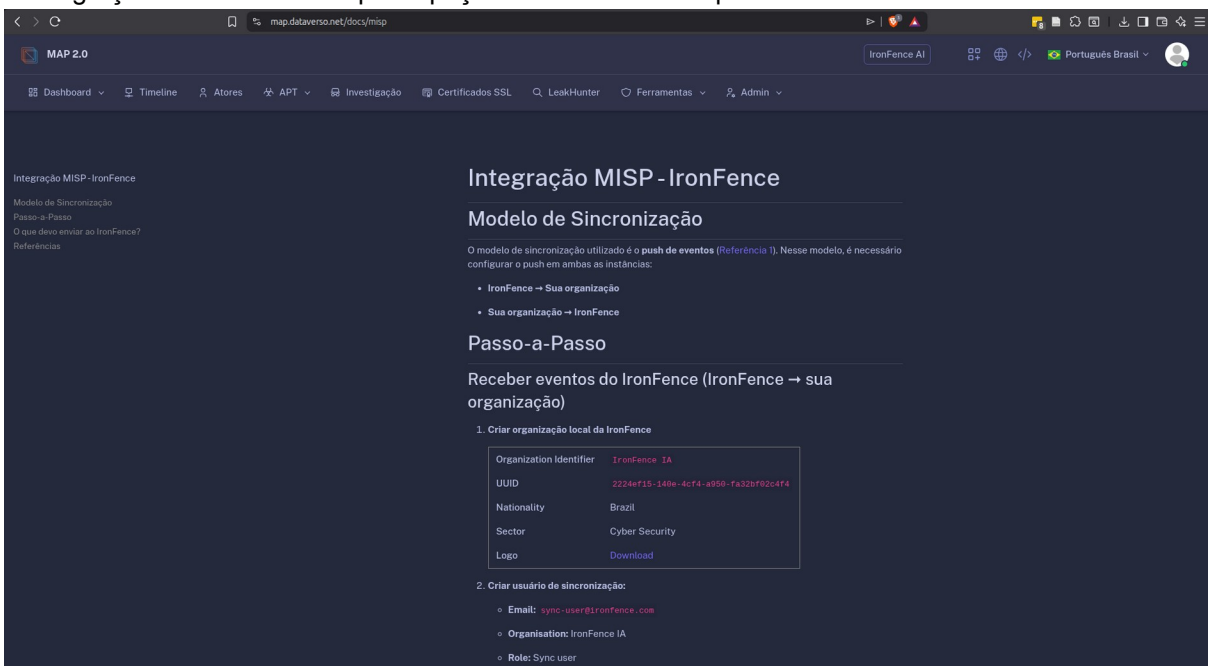


8.4. Incluir IoCs como hashes de malware, URLs maliciosas, IPs e domínios.
A plataforma coleta e disponibiliza hashes de malware, URLs maliciosas, IPs e domínios como IoCs padrão.

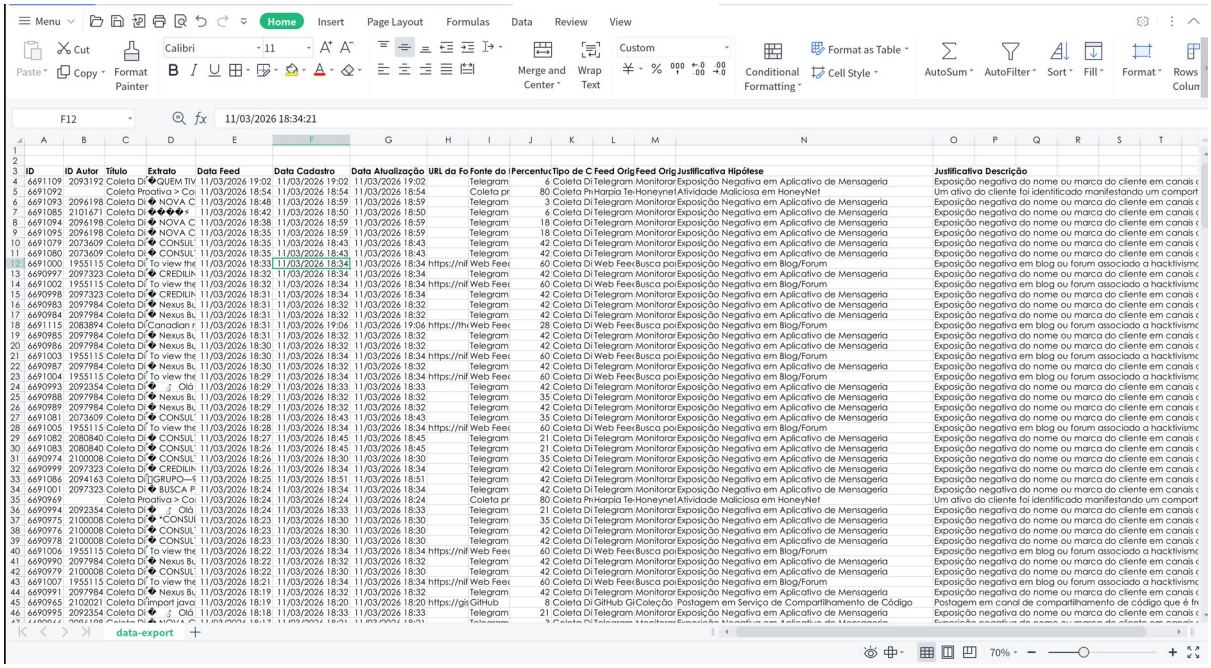


8.5. Participar de redes de compartilhamento de inteligência (ex.: ISACs, FS-ISAC).

A integração MISP viabiliza a participação em redes de compartilhamento.

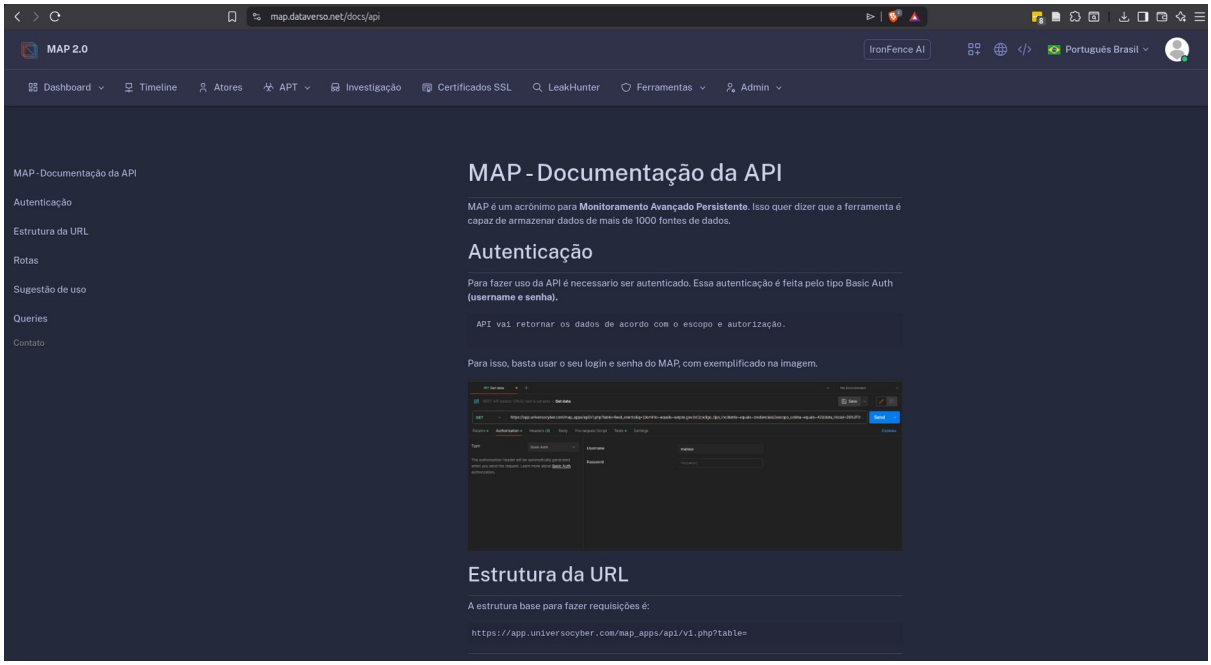


8.6. Fornecer IoCs com metadados, como nível de confiança e origem.
Os IoCs exportados incluem metadados como nível de confiança, origem da coleta e TTPs associados.



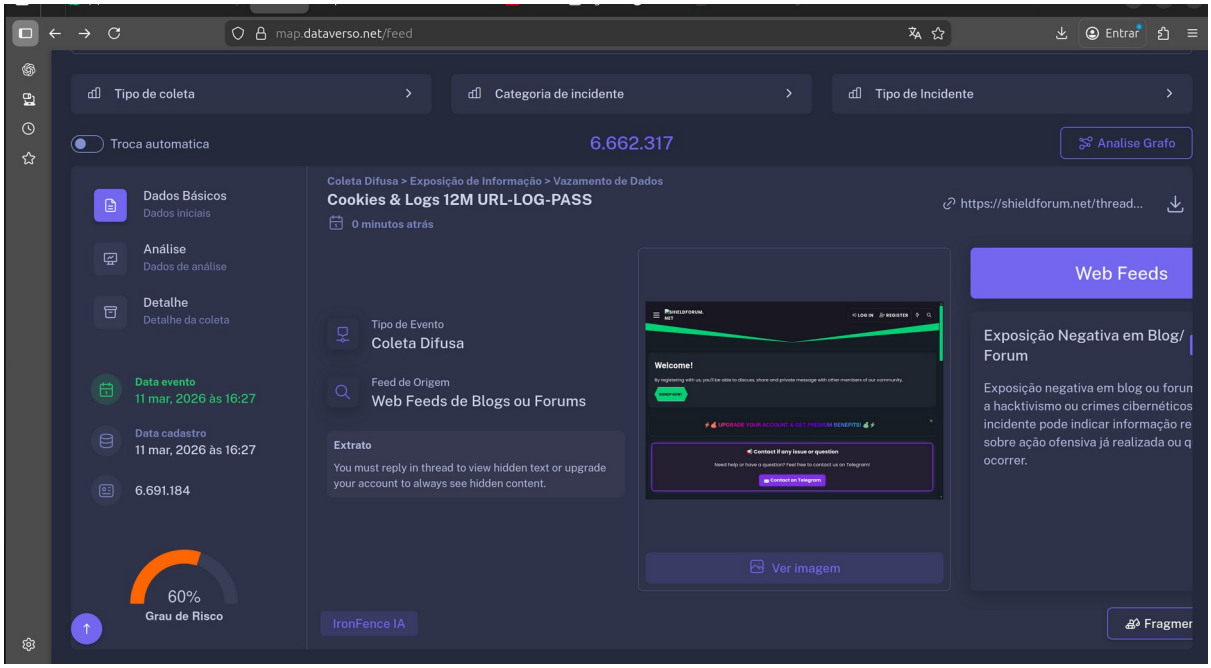
8.7. Garantir que IoCs sejam compatíveis com ferramentas de segurança do contratante.

A compatibilidade é garantida pelos formatos padronizados (STIX/TAXII, JSON, CSV) e pela API RESTful.



8.8. Atualizar IoCs regularmente com base em novas descobertas.

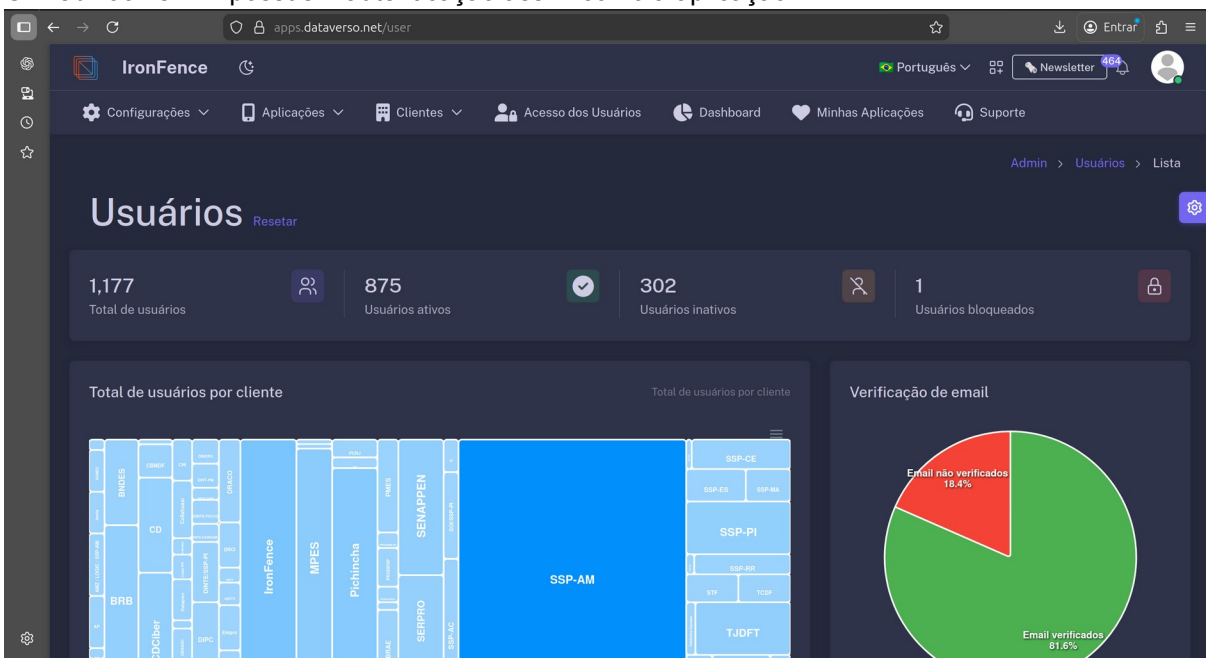
Os IoCs são atualizados automaticamente conforme novas coletas e análises são realizadas pela plataforma. Referência: https://map.dataverso.net/feed



8.9. Proteger IoCs compartilhados contra acesso não autorizado.

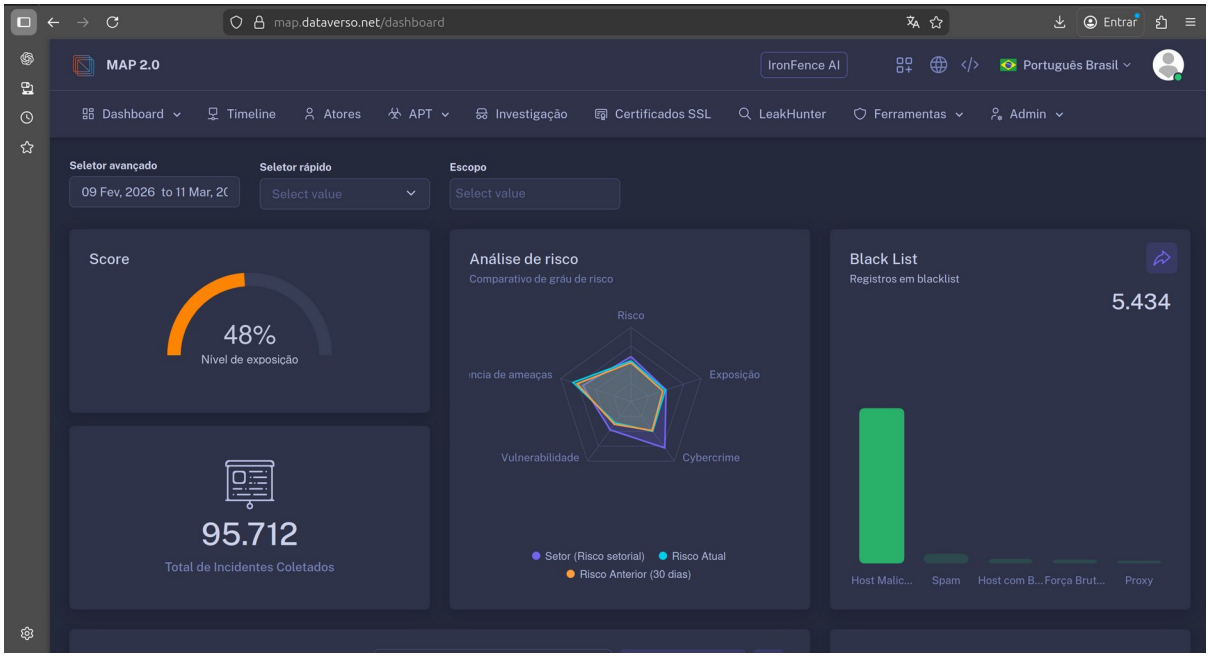
O acesso aos IoCs é protegido por autenticação, controle de permissões por usuário e transmissão criptografada via HTTPS.

O Webwook e API possuem autenticação assim como a aplicação.



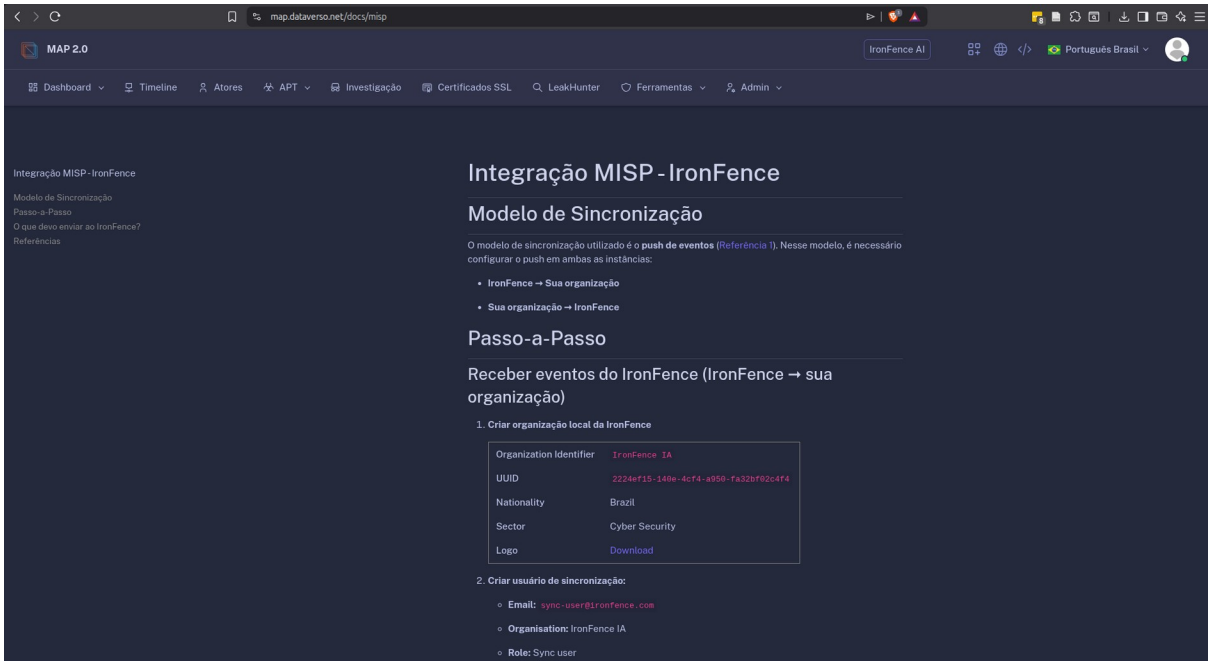
8.10. Fornecer relatórios sobre a utilização e eficácia dos IoCs compartilhados.

Dashboards e relatórios periódicos apresentam métricas de utilização e eficácia dos IoCs compartilhados. Referência: https://map.dataverso.net/docs/irc



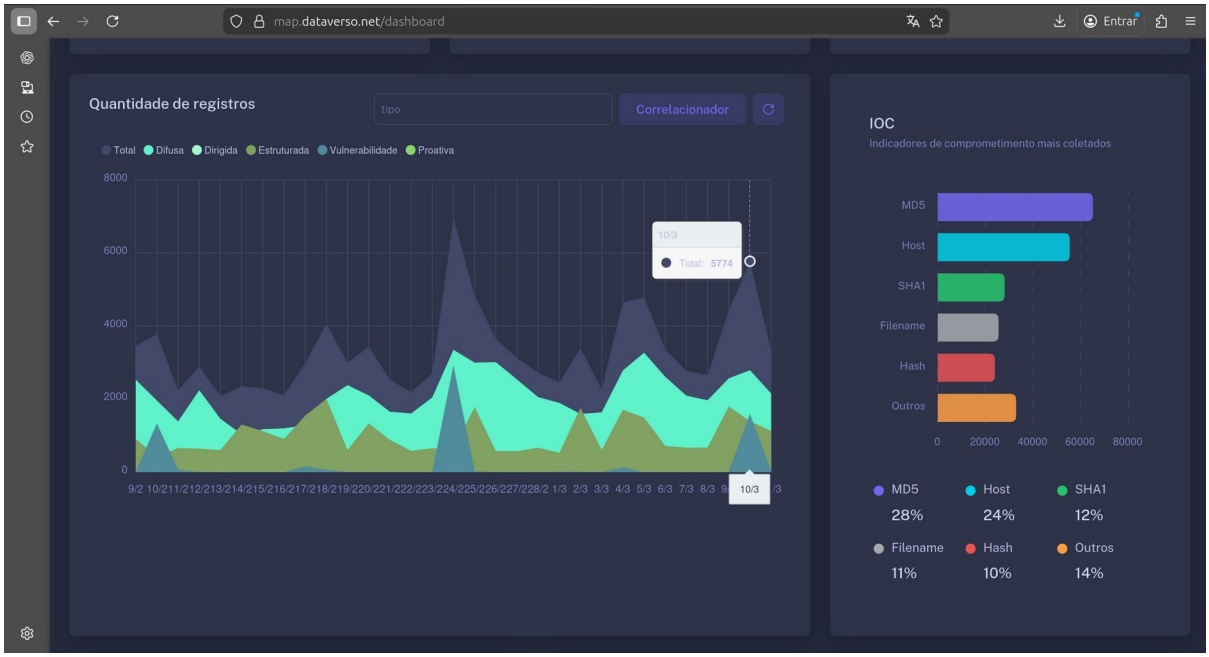
8.11. Integrar IoCs com feeds de inteligência de ameaças globais.

A integração com MISP e feeds globais de inteligência permite a correlação de IoCs internos com bases de ameaças mundiais. Referência: https://map.dataverso.net/docs/misp



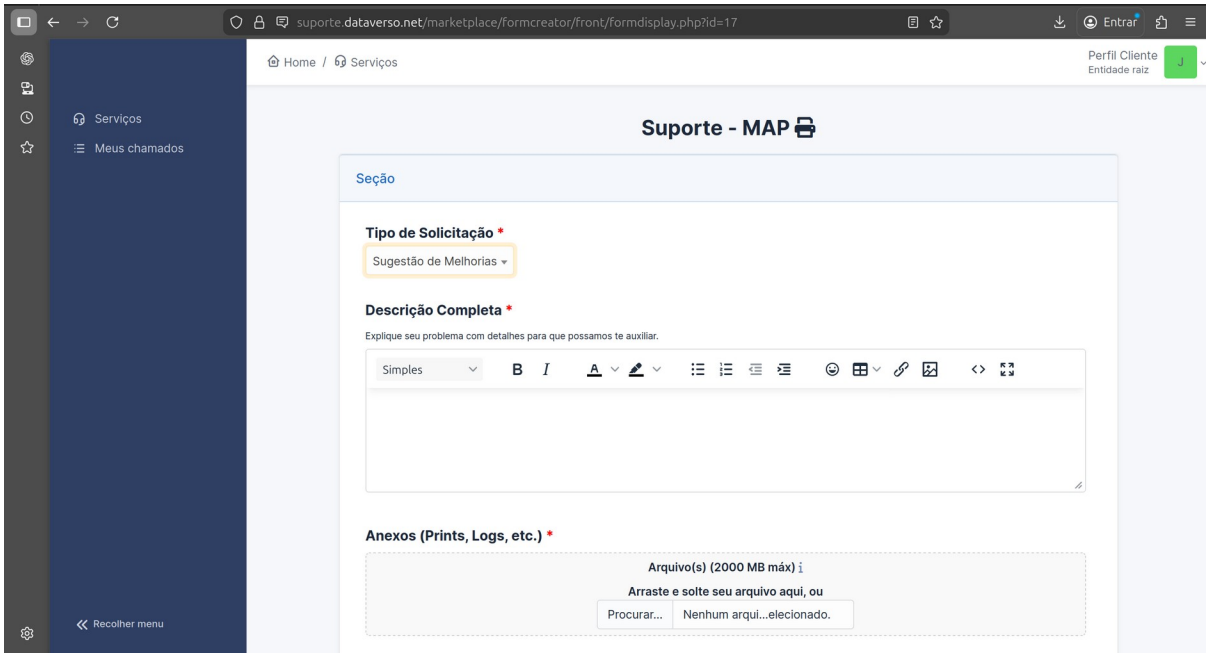
8.12. Garantir que IoCs sejam validados antes do compartilhamento.

Os IoCs passam por validação automatizada antes do compartilhamento, incluindo verificação de falsos positivos. Referência: https://map.dataverso.net/feed

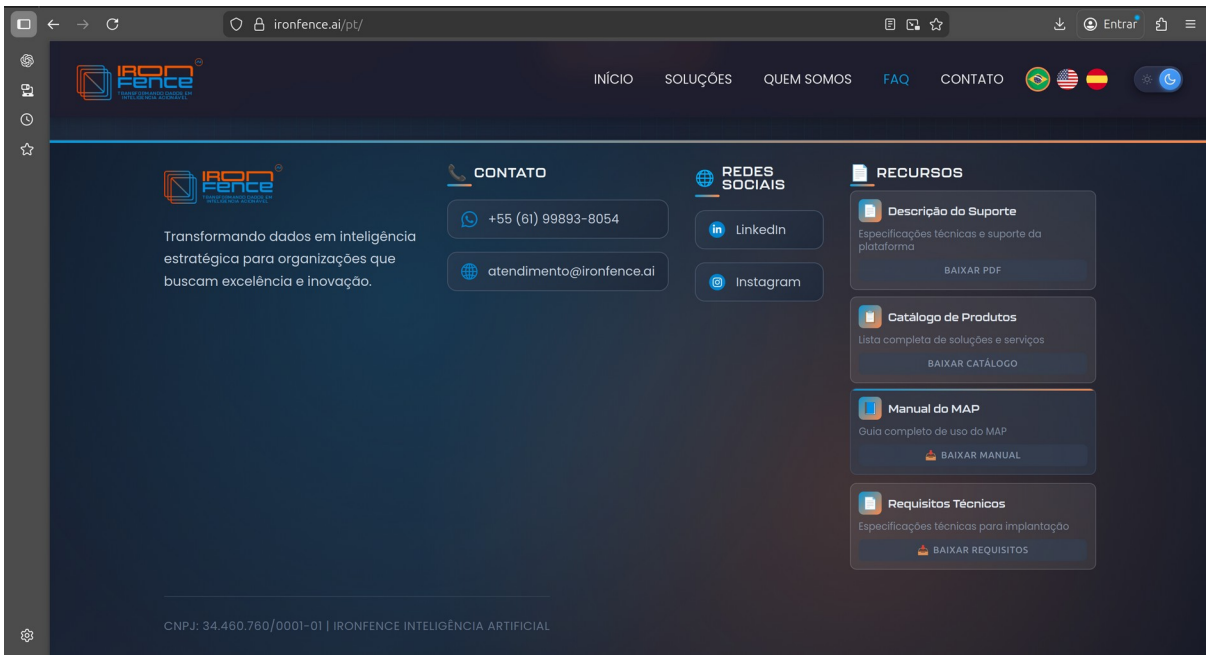


8.13. Oferecer suporte para personalização de IoCs com base em necessidades específicas.

A API permite personalização de consultas e filtros de IoCs conforme as necessidades específicas do BNB. Referência: https://map.dataverso.net/docs/api

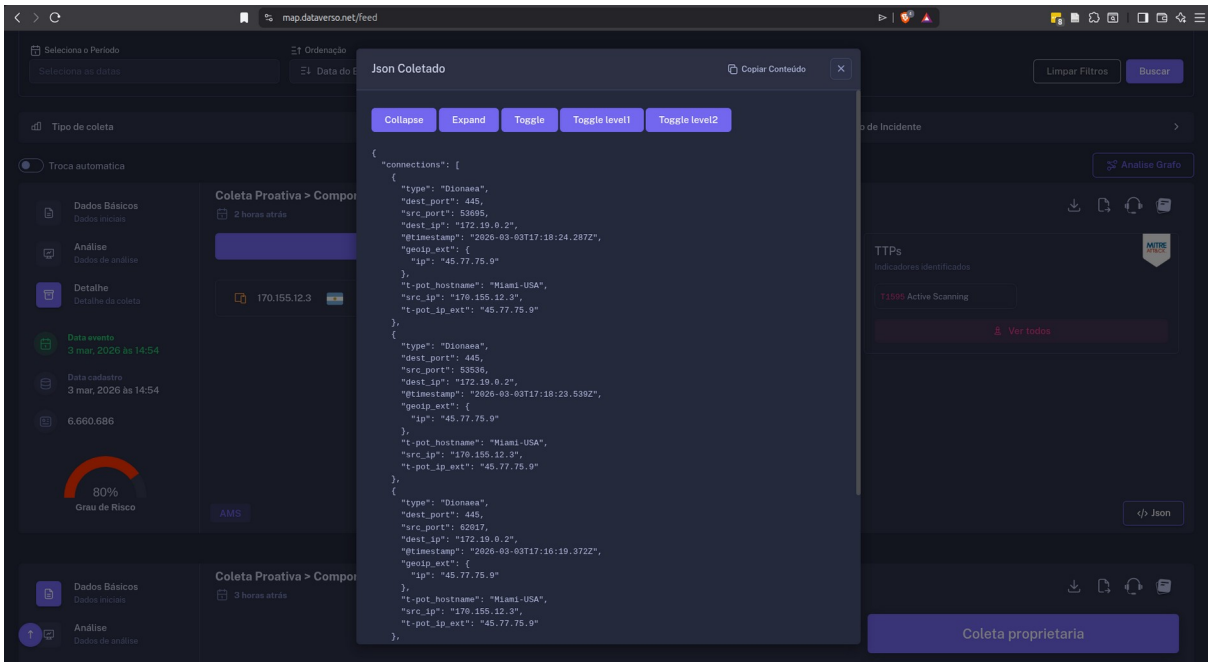


8.14. Fornecer documentação detalhada sobre o uso de IoCs fornecidos.

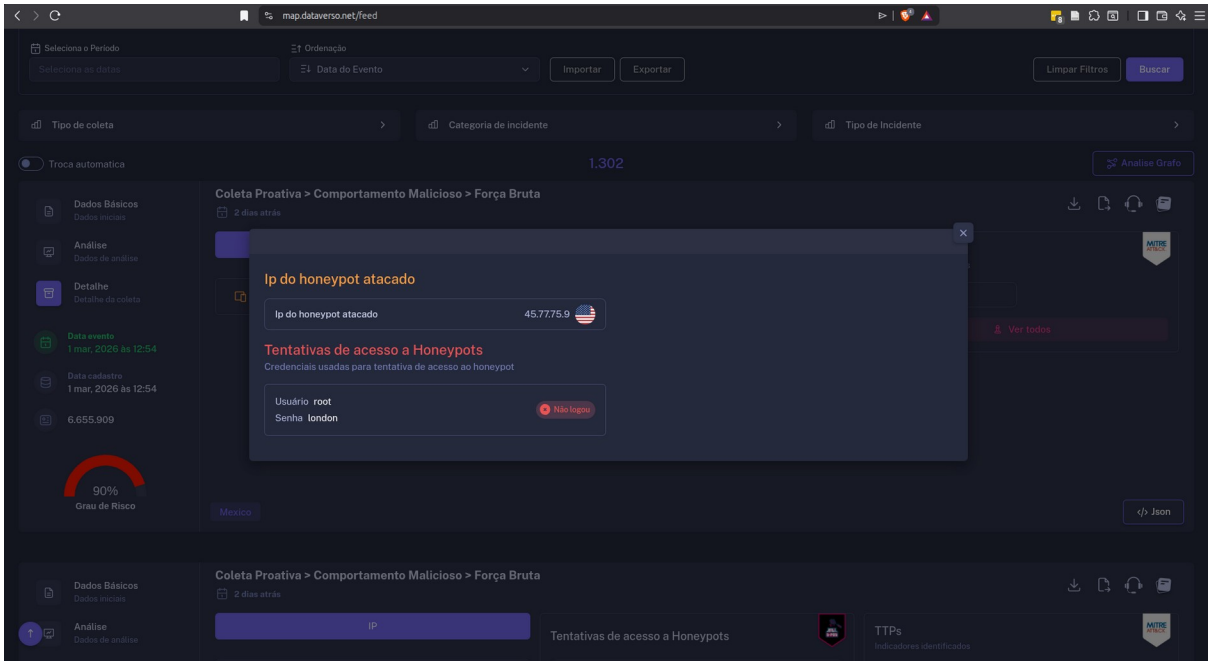


8.15. Garantir conformidade com regulamentações ao compartilhar IoCs sensíveis.

O controle é realizado a nível de usuário com as permissões de acesso.



Detalhes dos dados escaneados



Detalhes de tentativa de ataque

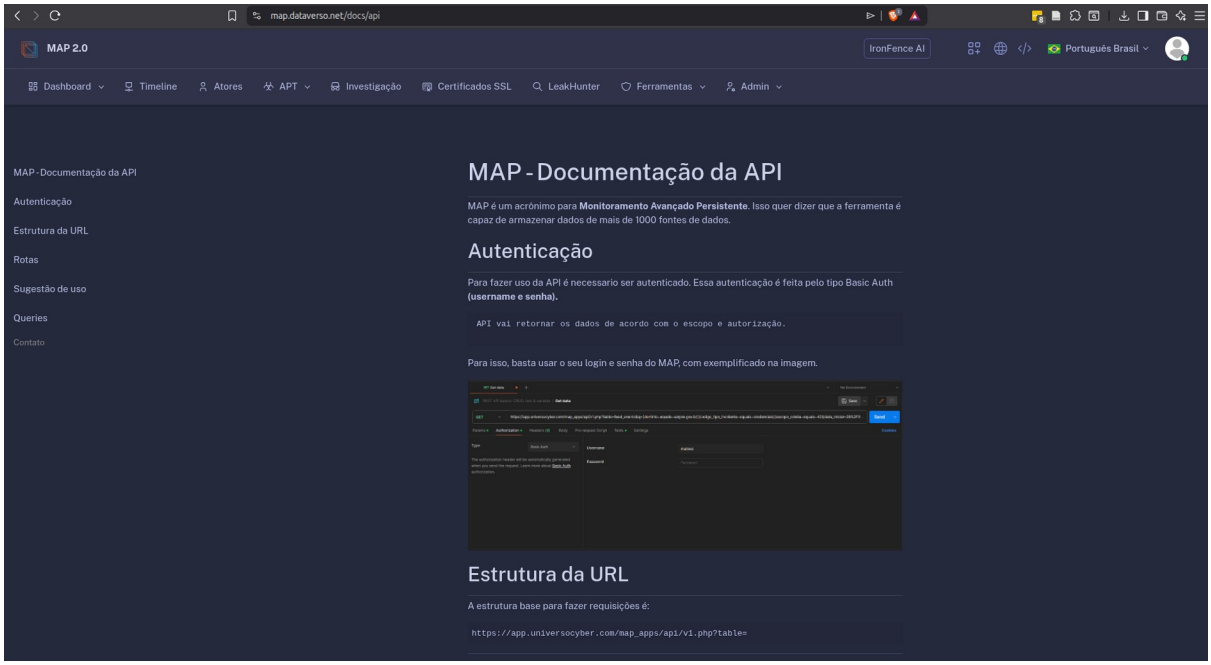
https://map.dataverso.net/sauron-dashboard

9. REQUISITOS DE INTEGRAÇÃO COM SIEM/SOAR

A plataforma MAP oferece integração com sistemas SIEM e SOAR através de Webhooks (https://map.dataverso.net/docs/webhook), MISP (https://map.dataverso.net/docs/misp) e API RESTful (https://map.dataverso.net/docs/api). Essas integrações permitem o envio automatizado de alertas, IoCs e eventos de inteligência para as ferramentas de segurança do CONTRATANTE.

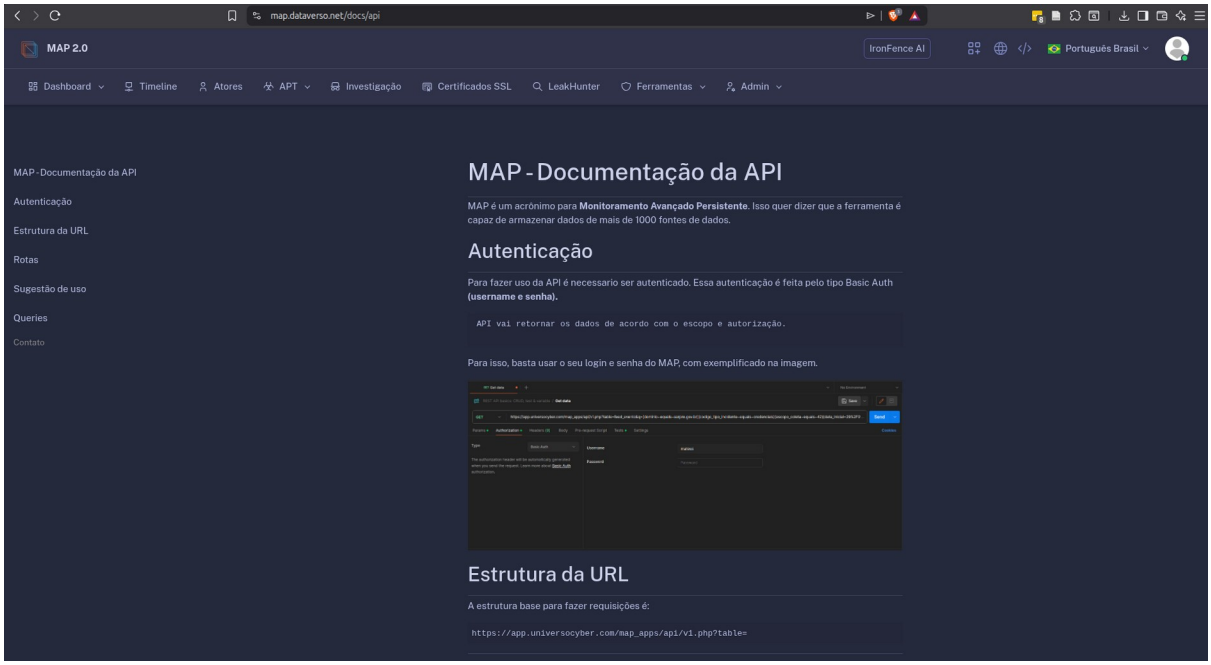
9.1. Integrar-se com sistemas SIEM populares (ex.: Splunk, QRadar, ArcSight).

A integração com SIEMs (Splunk, QRadar, ArcSight, entre outros) é feita via Webhooks e API RESTful, que enviam alertas e IoCs diretamente para os coletores do SIEM. Referência: https://map.dataverso.net/docs/webhook e https://map.dataverso.net/docs/api

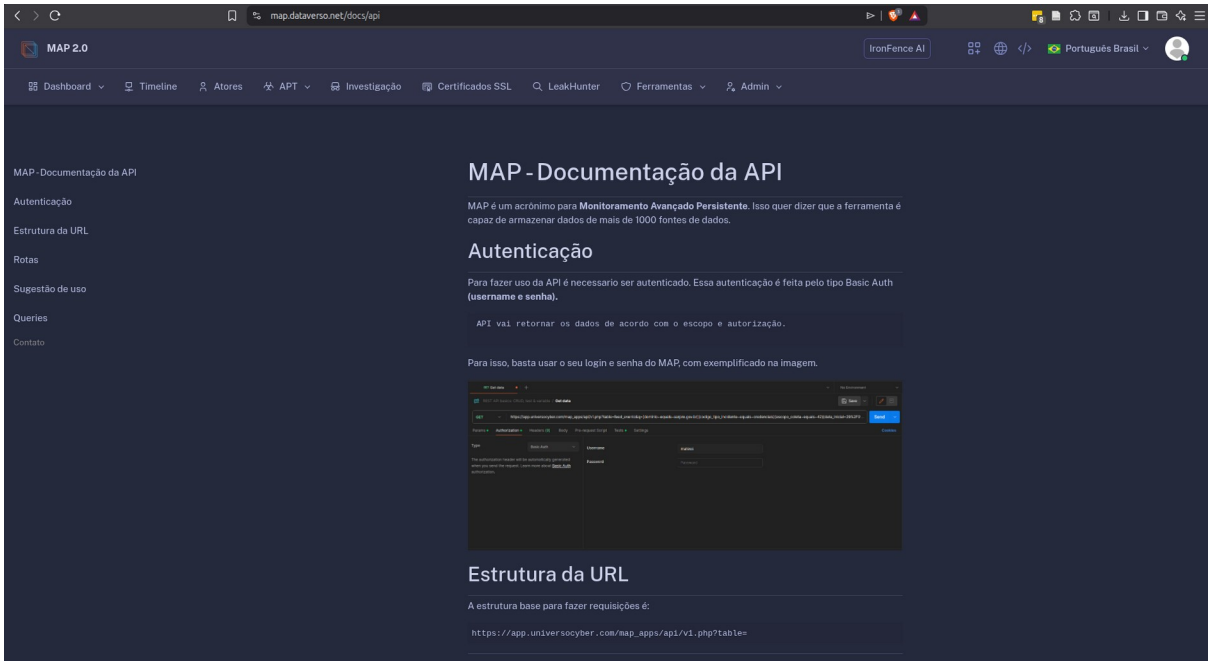


9.2. Suportar plataformas SOAR (ex.: Palo Alto Cortex XSOAR, ServiceNow).

Plataformas SOAR (Cortex XSOAR, ServiceNow, etc.) são suportadas via API RESTful e Webhooks, permitindo o acionamento automático de playbooks. Referência: https://map.dataverso.net/docs/api

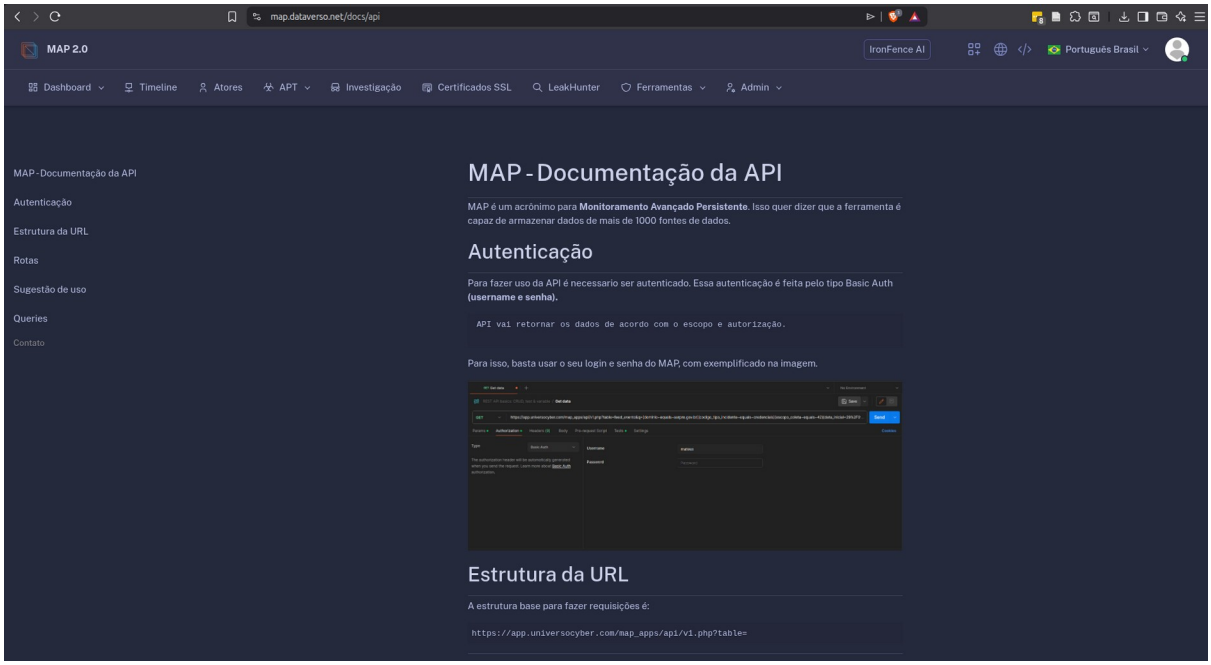


9.3. Fornecer APIs RESTful para integração com ferramentas de segurança existentes.
A API RESTful completa está documentada e disponível para integração com qualquer ferramenta de segurança. Referência: https://map.dataverso.net/docs/api


map.dataverso.net/docs/api
MAP 2.0
IronFence AI
Português Brasil
Dashboard
Timeline
Atores
APT
Investigação
Certificados SSL
LeakHunter
Ferramentas
Admin
MAP - Documentação da API
Autenticação
Estrutura da URL
Rotas
Sugestão de uso
Queries
Contato
MAP - Documentação da API
MAP é um acrônimo para Monitoramento Avançado Persistente. Isso quer dizer que a ferramenta é capaz de armazenar dados de mais de 1000 fontes de dados.
Autenticação
Para fazer uso da API é necessario ser autenticado. Essa autenticação é feita pelo tipo Basic Auth (username e senha).
API vai retornar os dados de acordo com o escopo e autorização.
Para isso, basta usar o seu login e senha do MAP, com exemplificado na imagem.
Estrutura da URL
A estrutura base para fazer requisições é:
https://app.universocyber.com/map_apps/api/v1.php?table=

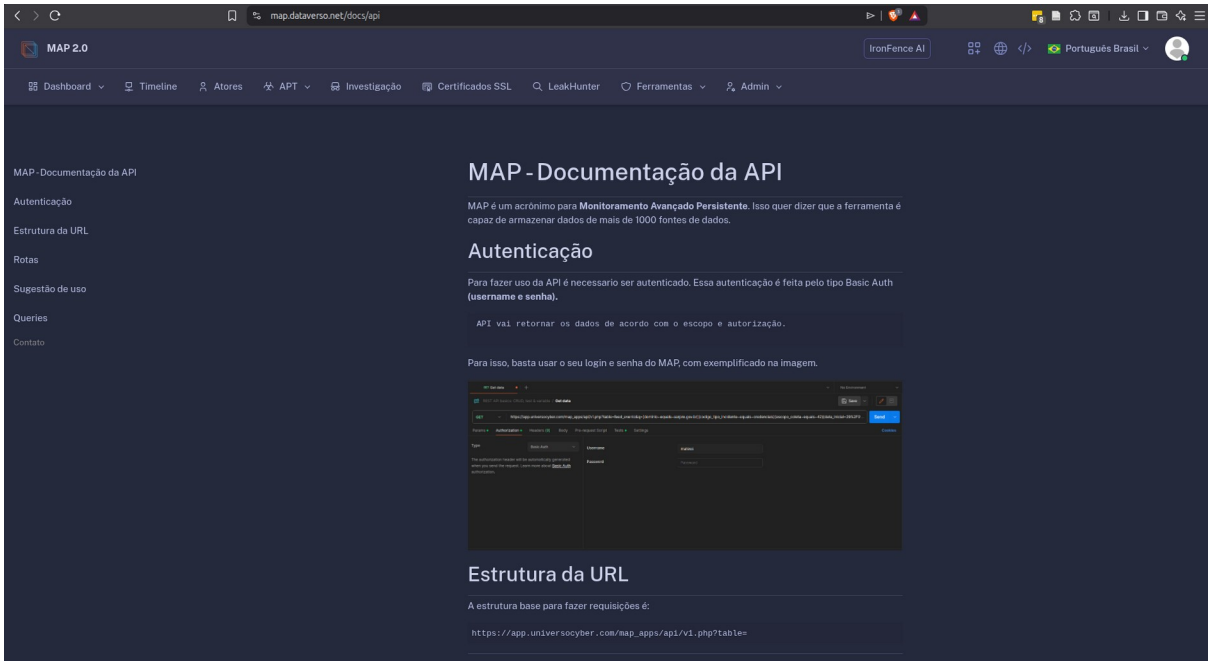
9.4. Garantir compatibilidade com formatos de log como CEF ou Syslog.

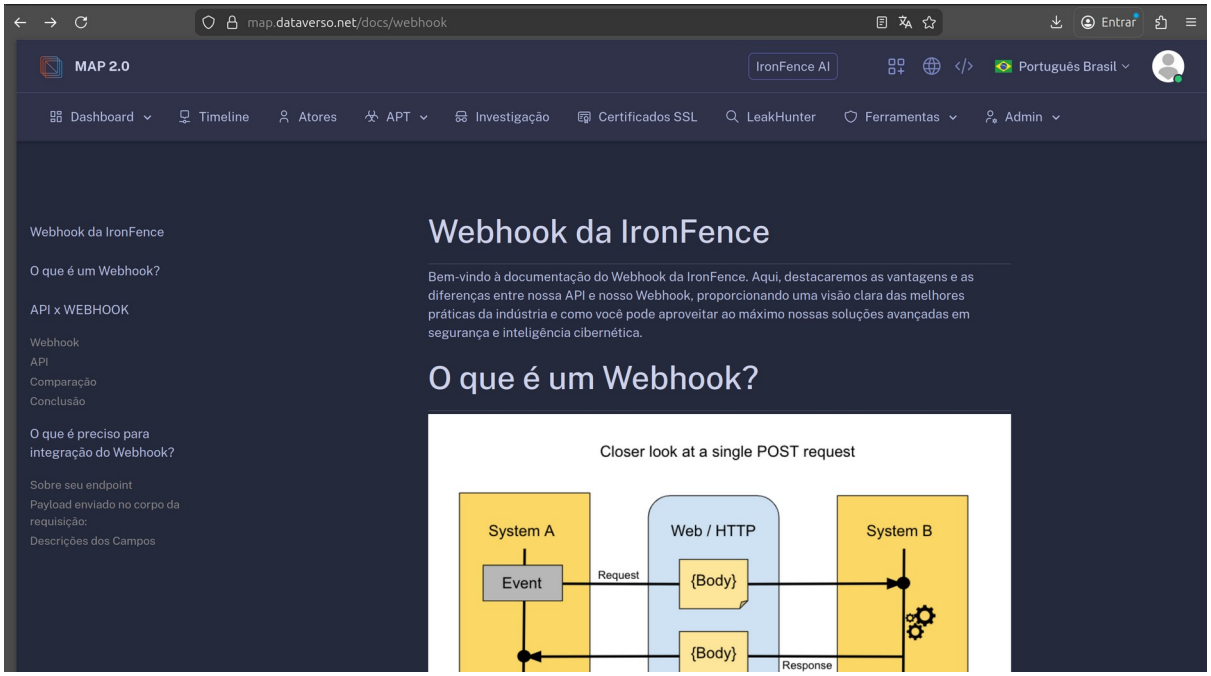
A API RESTful completa está documentada e disponível para integração com qualquer ferramenta de segurança. Referência: https://map.dataverso.net/docs/api



9.5. Suportar automação de respostas a incidentes via integração com SOAR.

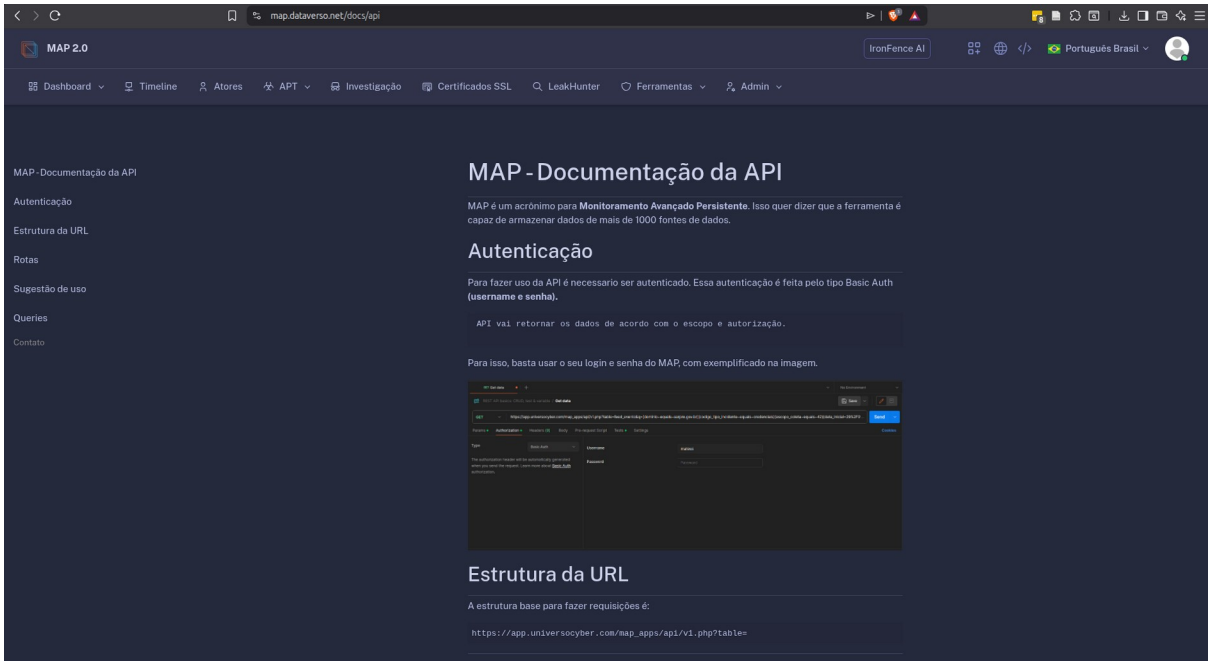
A integração com SOAR via API e Webhooks permite automação de respostas a incidentes, incluindo bloqueios, notificações e escalações. Referência: https://map.dataverso.net/docs/webhook e https://map.dataverso.net/docs/api



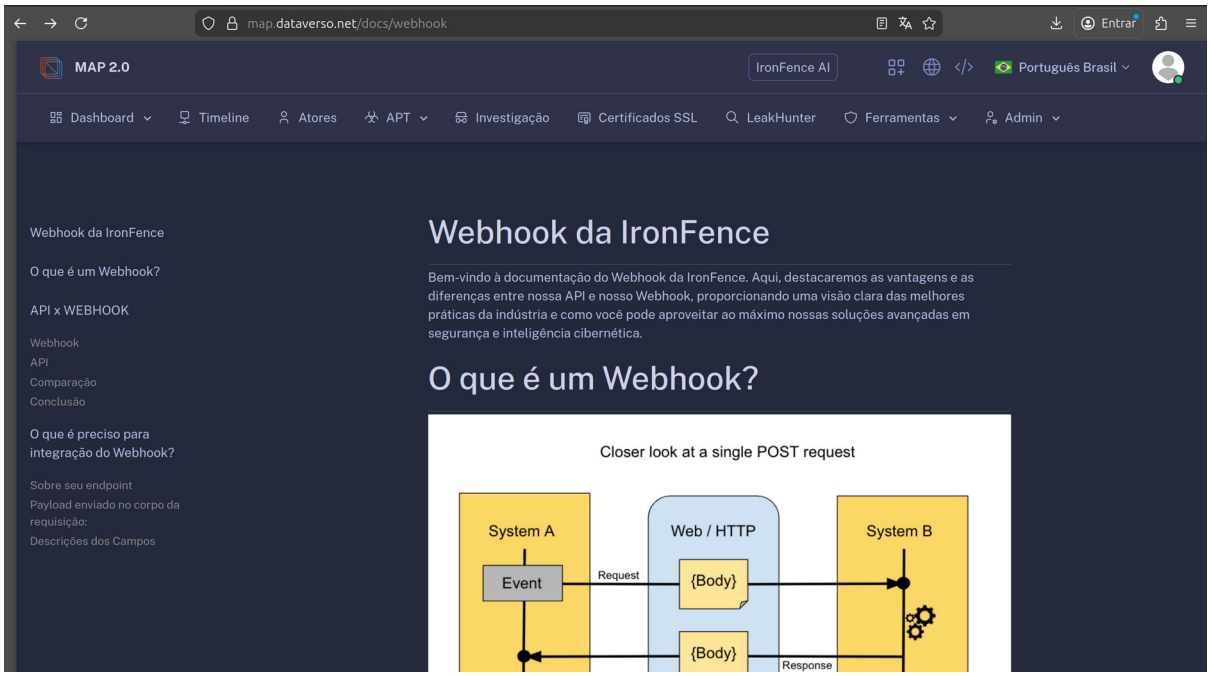


9.6. Fornecer playbooks pré-configurados para respostas a fraudes comuns.

A plataforma disponibiliza templates de integração que podem ser utilizados como base para playbooks de resposta a fraudes. Referência: https://map.dataverso.net/docs/api

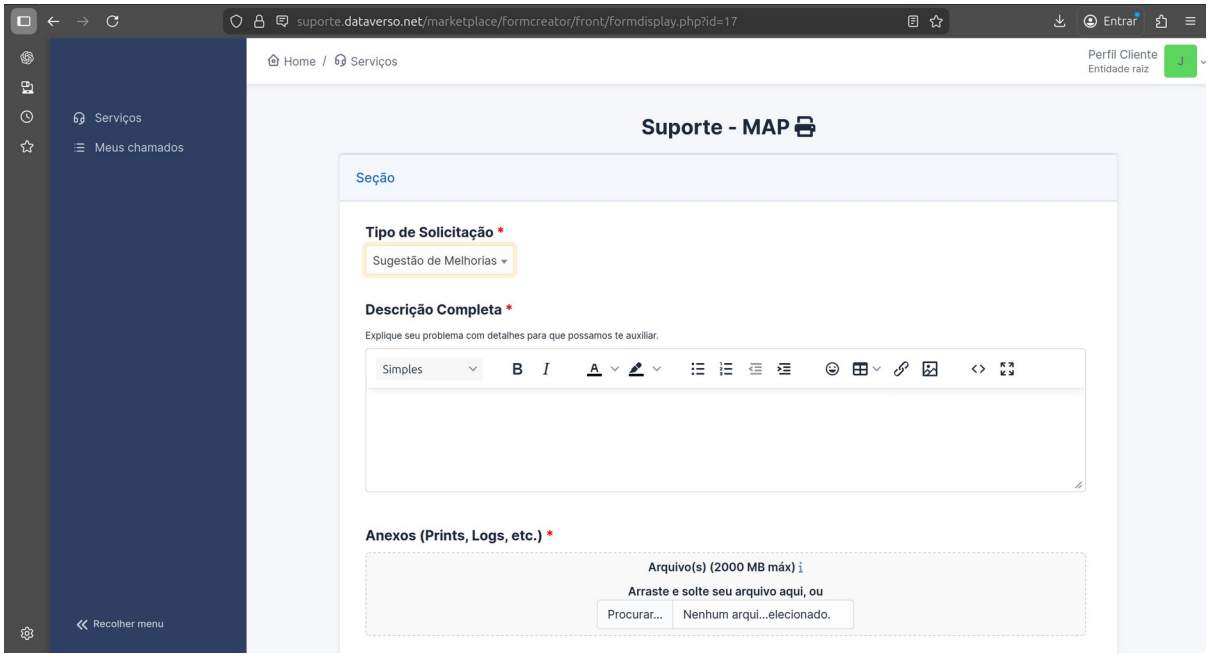


9.7. Garantir baixa latência na integração de dados com SIEM/SOAR.
As integrações operam com baixa latência, com Webhooks disparados em tempo real a cada nova detecção. Referência: https://map.dataverso.net/docs/webhook



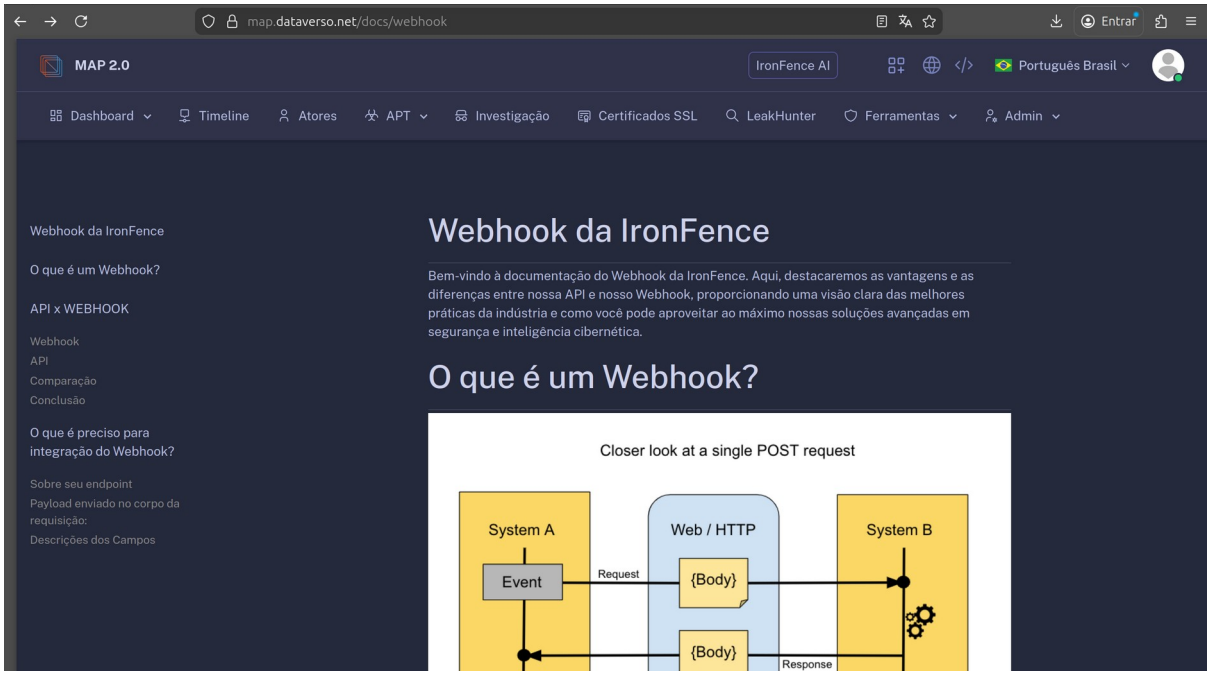
9.8. Oferecer suporte técnico para configuração inicial de integrações.

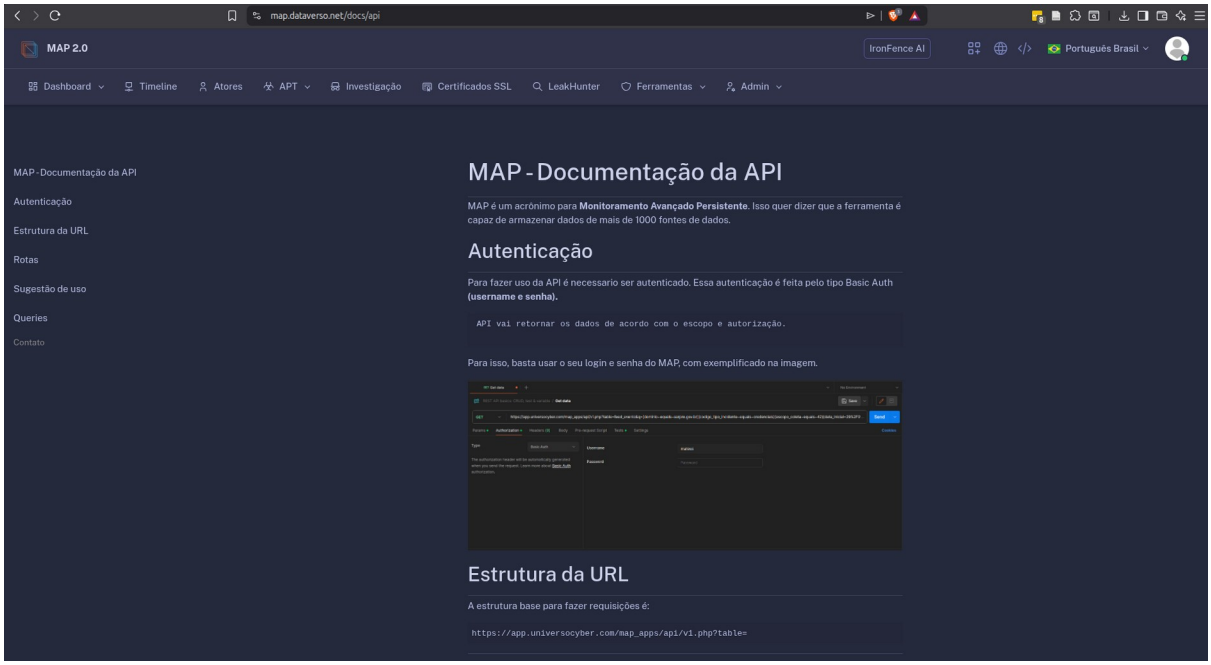
Suporte técnico dedicado é oferecido para a configuração inicial das integrações com o ambiente do CONTRATANTE. Referência: https://map.dataverso.net/docs/api

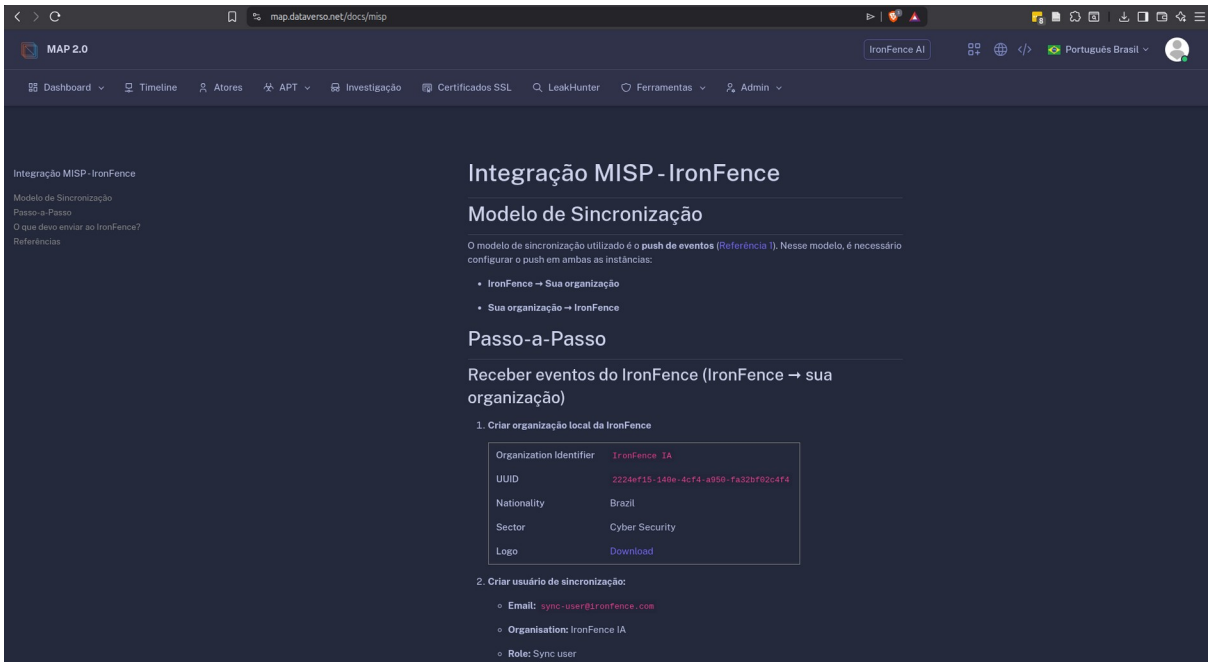


9.9. Fornecer documentação detalhada sobre APIs e integração.

documentação detalhada das APIs, Webhooks e integração MISP está disponível nos links: https://map.dataverso.net/docs/api, https://map.dataverso.net/docs/webhook e https://map.dataverso.net/docs/misp

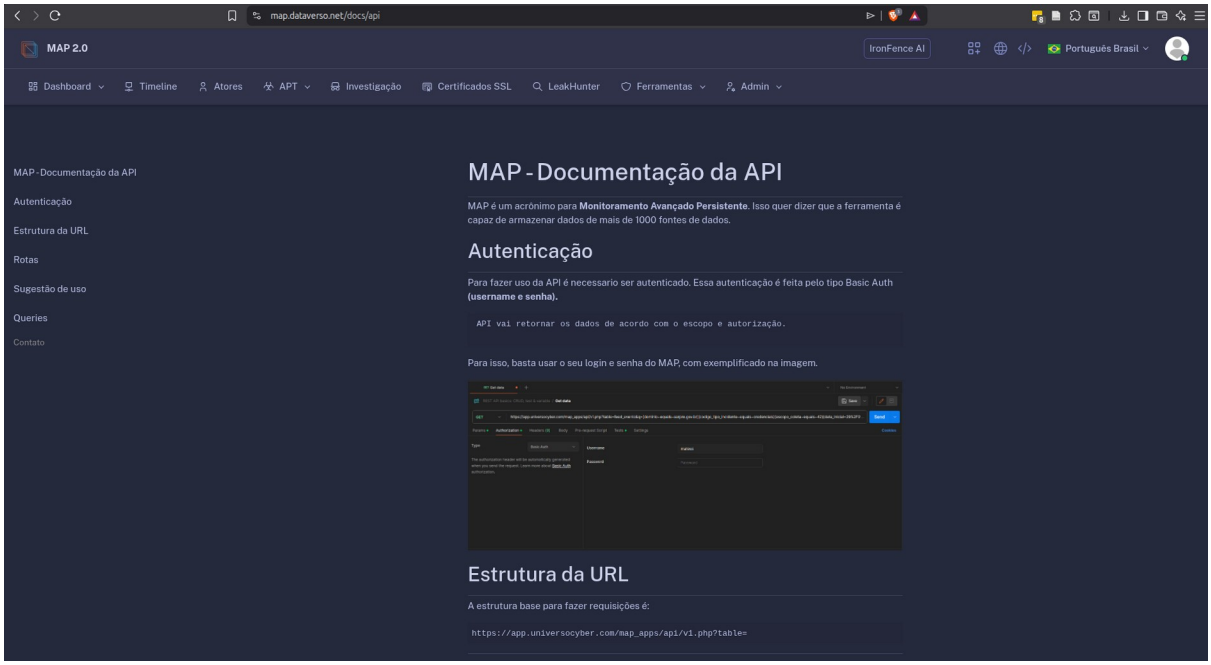






9.10. Garantir que dados enviados ao SIEM/SOAR sejam criptografados.

Todos os dados enviados às integrações SIEM/SOAR são transmitidos via HTTPS com TLS 1.2+, garantindo criptografia ponta a ponta. Referência: https://map.dataverso.net/docs/api



Integração com MISP, exportação nos formatos STIX e TAXII, além de API de integração (Vide documentos em anexo)