SEGURANÇA, INTELIGÊNCIA E DADOS

Manual Aplicação

MAP 2.0

INTRODUÇÃO

O MAP 2.0 é uma plataforma avançada para monitoramento e investigação de ameaças cibernéticas, fornecendo inteligência sobre vazamentos de dados, grupos APT, incidentes de segurança e atividades em mercados clandestinos. Ele centraliza diversas ferramentas para análise detalhada, permitindo a identificação de vulnerabilidades e ameaças em tempo real.

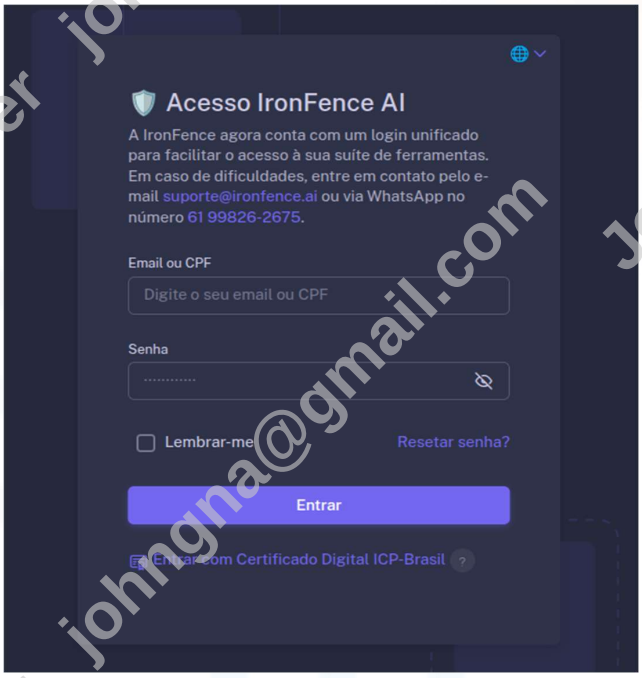
OBJETIVO

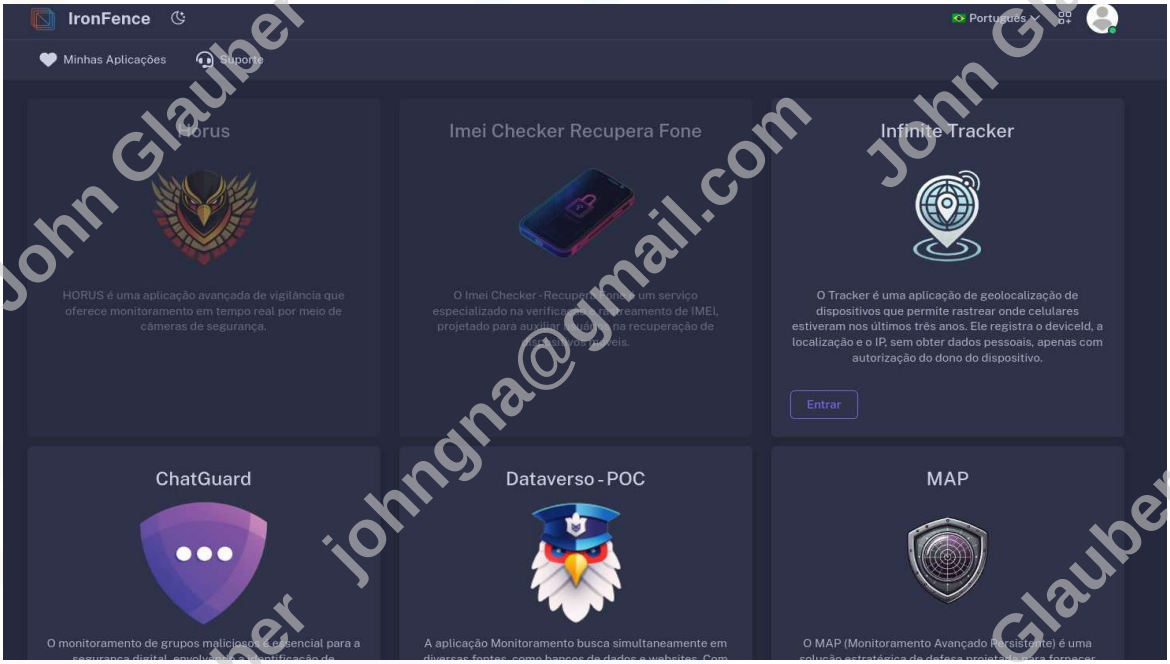
O MAP 2.0 tem como objetivo oferecer uma visão estratégica do cenário de ameaças cibernéticas, permitindo a análise de indicadores de comprometimento (IOCs), identificação de atores maliciosos e monitoramento de vazamentos. A plataforma auxilia na tomada de decisões, proporcionando insights valiosos para ações preventivas e investigativas.

ACESSO AO SISTEMA

Para acessar a plataforma, utilize o login unificado da **IronFence**:

1. Acesse: **https://apps.dataverso.net**.
2. Insira seu e-mail ou CPF e senha.
3. Clique em Entrar.
4. No painel de aplicações, selecione MAP 2.0.
5. Clique no botão Entrar e a aplicação será acessada automaticamente.
6. As aplicações que estiverem mais escuras são aquelas para as quais seu usuário não possui acesso.





DASHBOARD

O **Dashboard** do MAP 2.0 apresenta uma visão geral dos principais indicadores de segurança, oferecendo informações em tempo real sobre ameaças, vulnerabilidades e atividades suspeitas.

Abaixo estão descritas suas principais funcionalidades:

1. Filtros de Data

- **Seletor Avançado:** permite escolher um intervalo de datas específico para visualizar os dados coletados no período desejado.
- **Seletor Rápido:** oferece opções pré-definidas para seleção rápida de períodos (ex: Últimos 7 dias, Último mês).

2. Score de Exposição

- Exibe o **nível de exposição atual** em formato de velocímetro.
- O percentual indica o grau de vulnerabilidade da organização com base nos dados coletados.

3. Total de Incidentes Coletados

- Mostra o **número total de incidentes** registrados na plataforma.
- Ajuda a identificar o volume de eventos de segurança monitorados.

4. Blacklist (Registros em Blacklist)

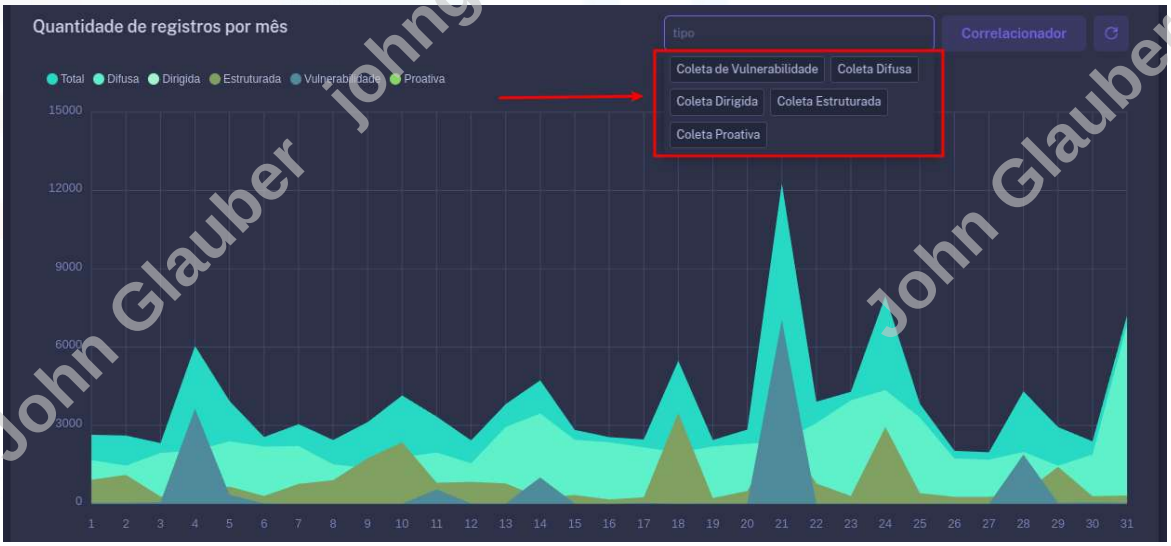
- Exibe o número de registros identificados em listas negras.
- Mostra a distribuição por categorias, como **Tentativas de Ataque**, **Hosts Maliciosos**, **Spam**, entre outros.

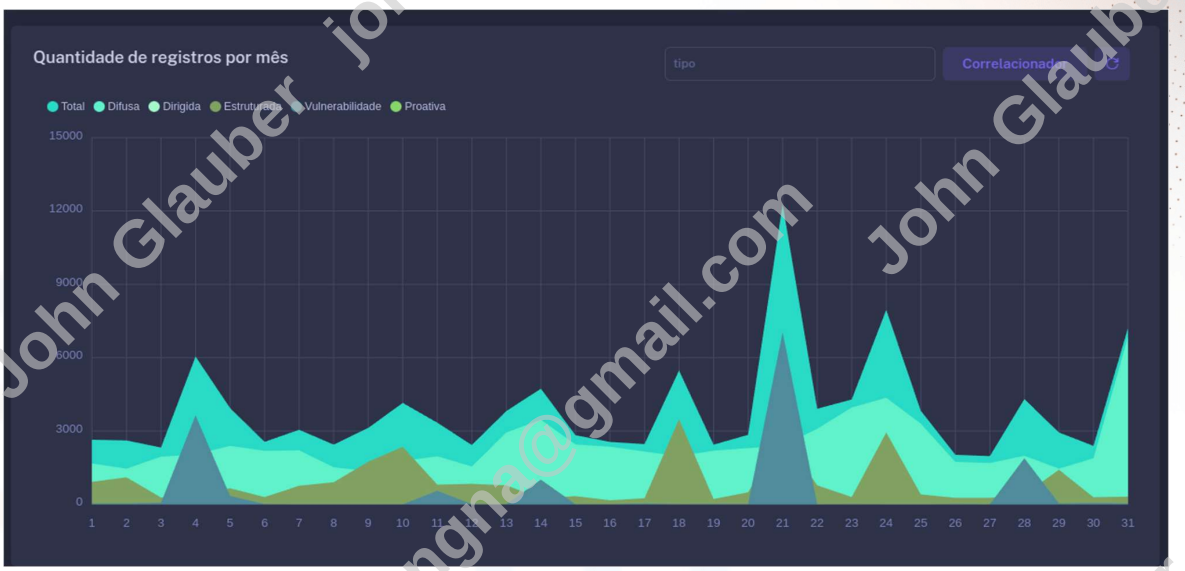
Botão de Detalhamento: o ícone de seta é um redirecionador para a Timeline, utilizando filtros específicos para exibir apenas registros de blacklist.

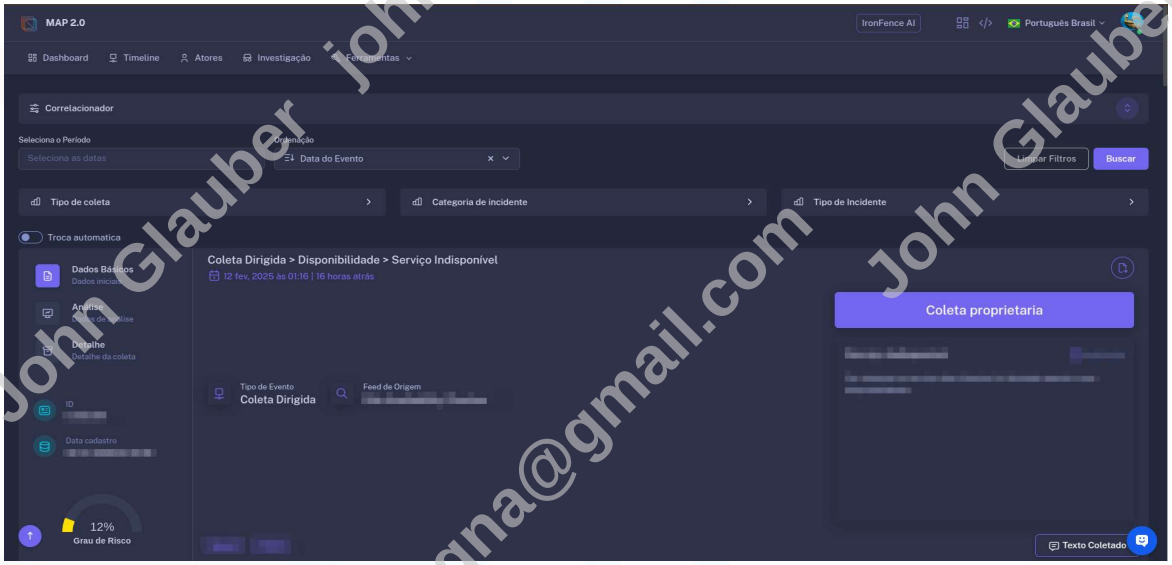
5. Quantidade de Registros por Mês

- Gráfico de linha demonstrando a evolução da quantidade de registros coletados ao longo dos meses.
- Filtros para segmentação por tipo de coleta: **Difusa**, **Dirigida**, **Estruturada**, **Vulnerabilidade**, **Proativa**.

Correlacionador: após selecionar o tipo de coleta, clique no botão "Correlacionador" para visualizar dados detalhados e correlações.



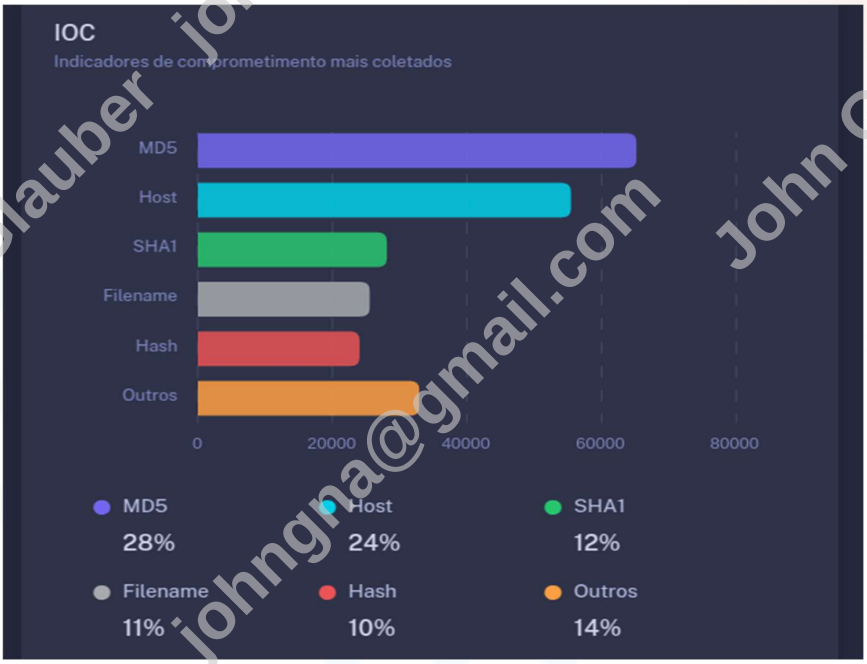




6. IOC (Indicadores de Comprometimento)

- Apresenta os **indicadores mais coletados**, como **MD5**, **Host**, **SHA1**, entre outros.
- O gráfico de barras facilita a visualização da predominância de cada tipo de IOC.

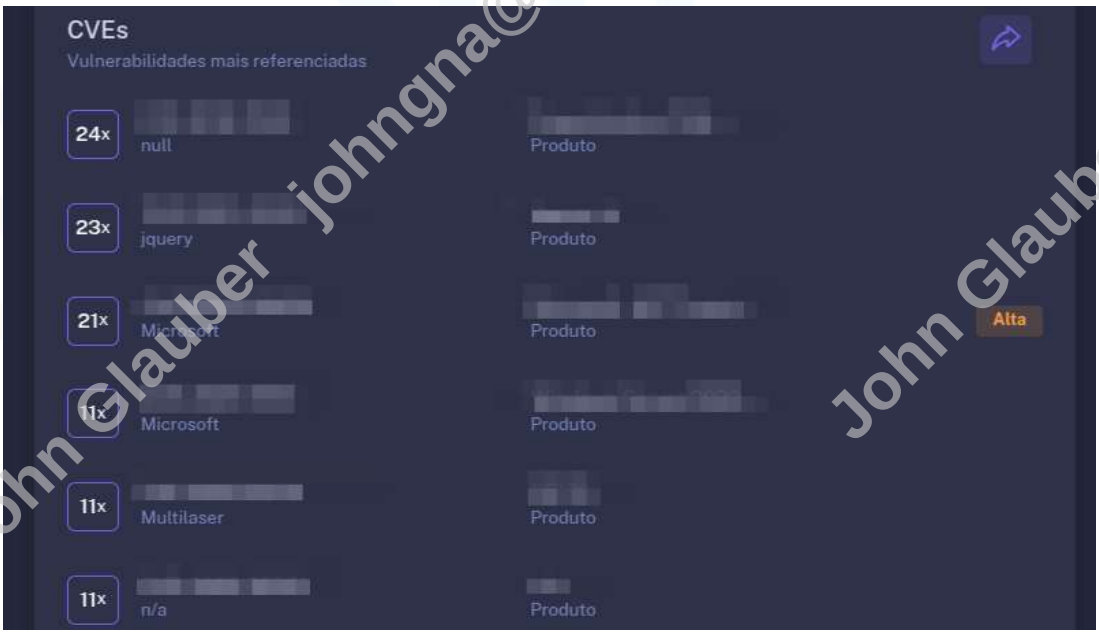
Botão de Detalhamento: o ícone de seta é um redirecionador para a Timeline, utilizando filtros específicos para exibir apenas os IOCs coletados.



7. CVEs (Vulnerabilidades Referenciadas)

- Lista as vulnerabilidades mais mencionadas, identificadas por seus códigos **CVE**.
- Detalha o produto afetado e o nível de criticidade (ex: **Média**, **Crítica**).

Botão de Detalhamento: o ícone de seta é um redirecionador para a Timeline, utilizando filtros específicos para exibir apenas informações detalhadas sobre CVEs.



8. Ativos Expostos

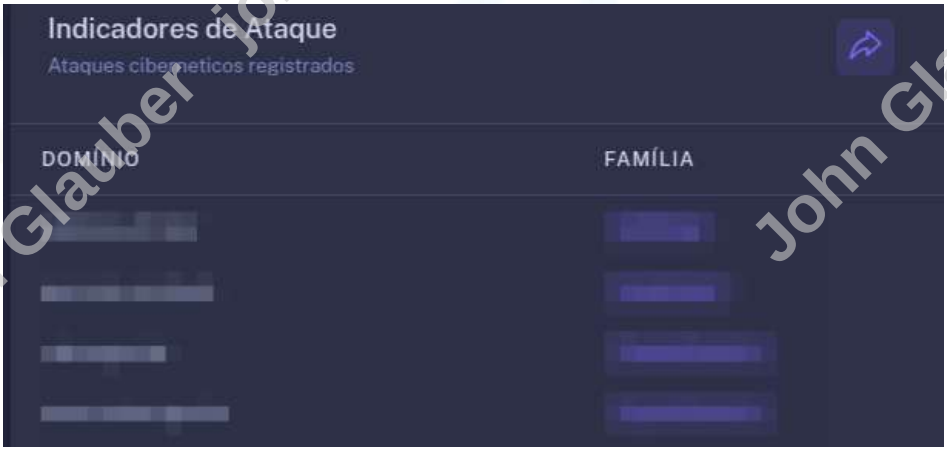
- Mostra o total de ativos vulneráveis identificados.
- Classificação por severidade: **Crítica**, **Alta**, **Moderada**.
- Lista de **últimos registros** com detalhes do ativo e sua vulnerabilidade.

Botão de Detalhamento: o ícone de seta é um redirecionador para a Timeline, utilizando filtros específicos para exibir apenas os ativos expostos.

9. Indicadores de Ataque

- Tabela com domínios associados a atividades maliciosas.
- Classificação por famílias de ameaças (ex: **Suspicious**, **Symmi.Generic**).

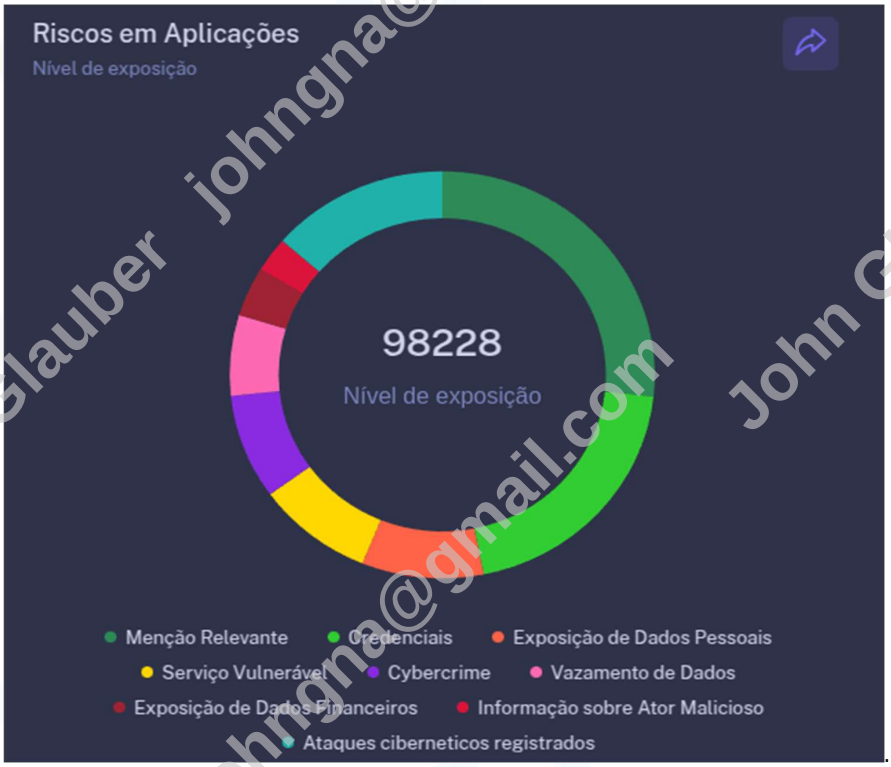
Botão de Detalhamento: o ícone de seta é um redirecionador para a Timeline, utilizando filtros específicos para exibir apenas os ataques cibernéticos registrados.



10. Riscos em Aplicações

- Gráfico de pizza ilustrando a distribuição dos diferentes tipos de riscos em aplicações.
- Inclui categorias como **Credenciais Vazadas**, **Exposição de Dados Pessoais**, **Cybercrime**, entre outros.

Botão de Detalhamento: o ícone de seta é um redirecionador para a Timeline, utilizando filtros específicos para exibir apenas os riscos relacionados a aplicações.



11. Vazamentos

- Lista os vazamentos de dados mais recentes.
- Informa a origem do vazamento (ex: **Telegram**, **WhatsApp**) e o tipo de dado comprometido (ex: **Credenciais**).

Botão de Detalhamento: o ícone de seta é um redirecionador para a Timeline, utilizando filtros específicos para exibir apenas os vazamentos identificados.

12. Atividades de Atores Maliciosos

- Exibe os atores maliciosos mais ativos e suas motivações (ex: **Ransomware**, **Espionagem**, **Hacktivismo**).
- Inclui um gráfico de barras com o número de registros por ator.

Botão de Detalhamento: o ícone de seta é um redirecionador para a Timeline, utilizando filtros específicos para exibir apenas as atividades dos atores maliciosos.

13. HoneyNet (Mapa de Ataques)

- Mapa global interativo com a geolocalização dos ataques cibernéticos registrados.
- Cada ponto vermelho representa uma ocorrência, com a quantidade de incidentes por região.

Botão de Detalhamento: o ícone de seta é um redirecionador para a Timeline, utilizando filtros específicos para exibir apenas os ataques cibernéticos registrados.

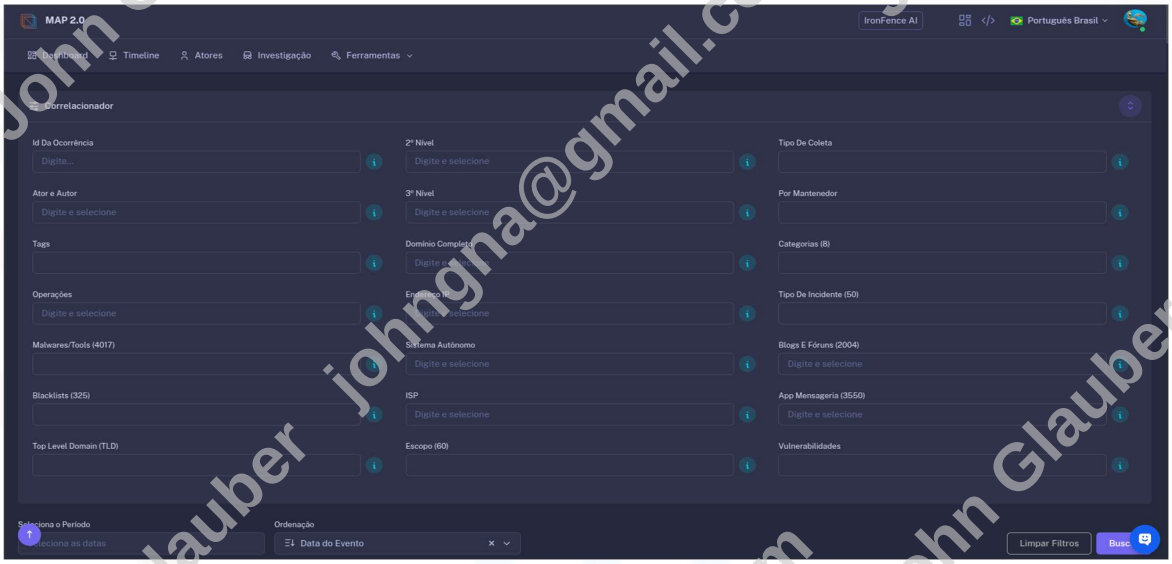
TIMELINE

A **Timeline** do MAP 2.0 é a seção responsável por exibir os registros detalhados de incidentes, permitindo que os usuários analisem eventos específicos com base em filtros avançados. Ela organiza e apresenta informações sobre ameaças, vulnerabilidades e atividades suspeitas de maneira clara e acessível.

1. Correlacionador

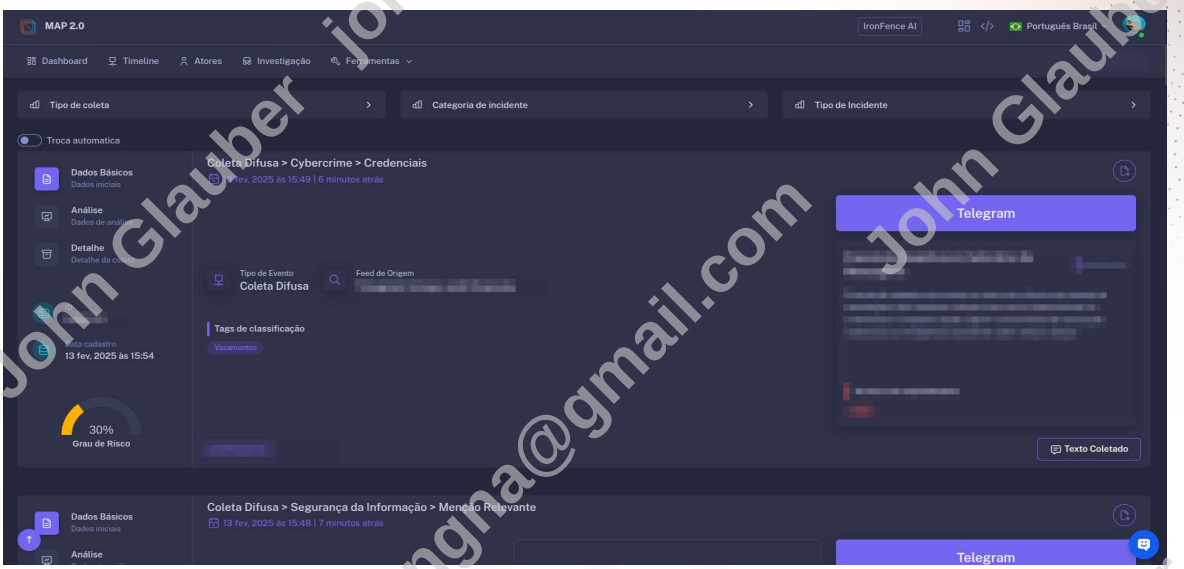
- O **Correlacionador** é a ferramenta utilizada para refinar buscas e aplicar filtros avançados.
- Permite pesquisar por diversos critérios, como **ID da Ocorrência, Tipo de Coleta, Endereço IP, Blacklists, Tags, Categorias de Incidente**, entre outros.

- Cada campo possui um ícone de informação ("i") que explica sua funcionalidade e como utilizá-lo corretamente.
- Os usuários podem **limpar filtros** ou **executar uma busca** para encontrar registros específicos.



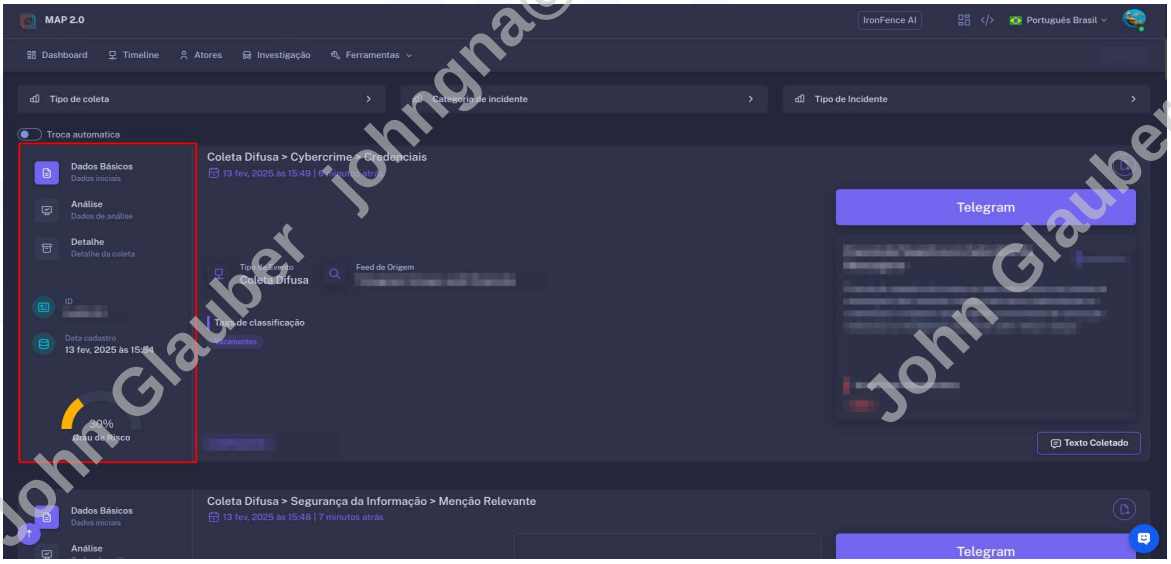
2. Exibição de Resultados na Timeline

- Os resultados são exibidos em formato de **cartões de incidente**, cada um contendo detalhes relevantes sobre a coleta realizada.
- Os incidentes são organizados cronologicamente e podem conter informações como:
  - **Tipo de Evento** (Ex: Coleta Estruturada, Coleta Difusa, Coleta Proativa).
  - **Feed de Origem**, indicando a fonte dos dados coletados.
  - **Tags de Classificação**, que ajudam na categorização do incidente.
  - **Justificativa**, trazendo explicações adicionais sobre a ameaça ou evento.
  - **Termos Correspondentes**, que destacam palavras-chave encontradas nos dados coletados.
  - **Grau de Risco**, exibido em uma barra visual indicando a criticidade do incidente.



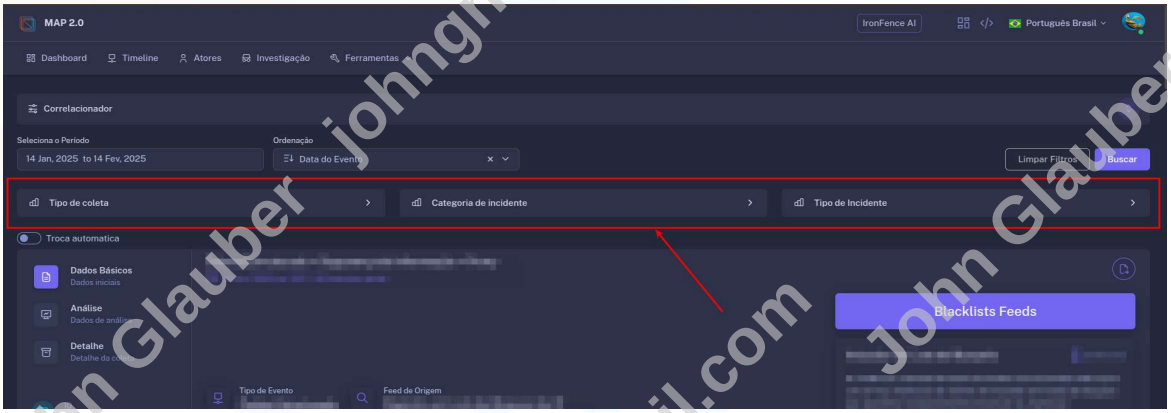
3. Detalhamento do Incidente

- Cada incidente pode ser expandido para exibir **dados básicos, análises e detalhes da coleta**.
- Informações importantes incluem:
  - **ID do Incidente** e **Data de Cadastro**.
  - **Detalhes do evento e de sua fonte**.
  - **Imagens ou fragmentos de texto coletados**.



4. Filtros de Pesquisa

- A **Timeline** permite buscar e filtrar incidentes de forma precisa através de:
    - **Tipo de Coleta**
    - **Categoria de Incidente**
    - **Tipo de Incidente**
    - **Tags e Palavras-chave**
- Esses filtros podem ser combinados para refinar ainda mais a busca.

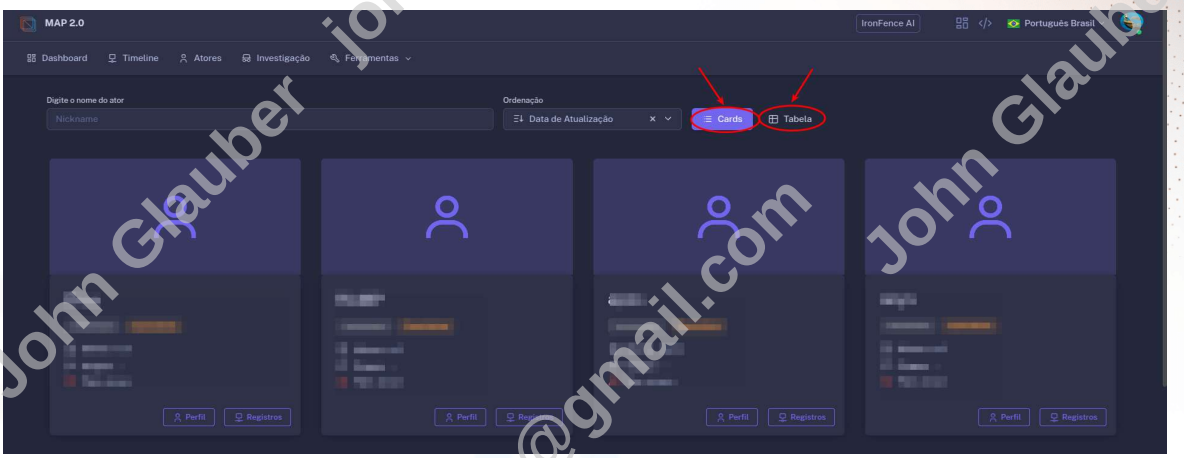


ATORES

A tela de **Atores** permite visualizar grupos e indivíduos envolvidos em atividades maliciosas, com informações detalhadas sobre suas motivações, idioma, origem e registros de incidentes.

1. Visualizações Disponíveis

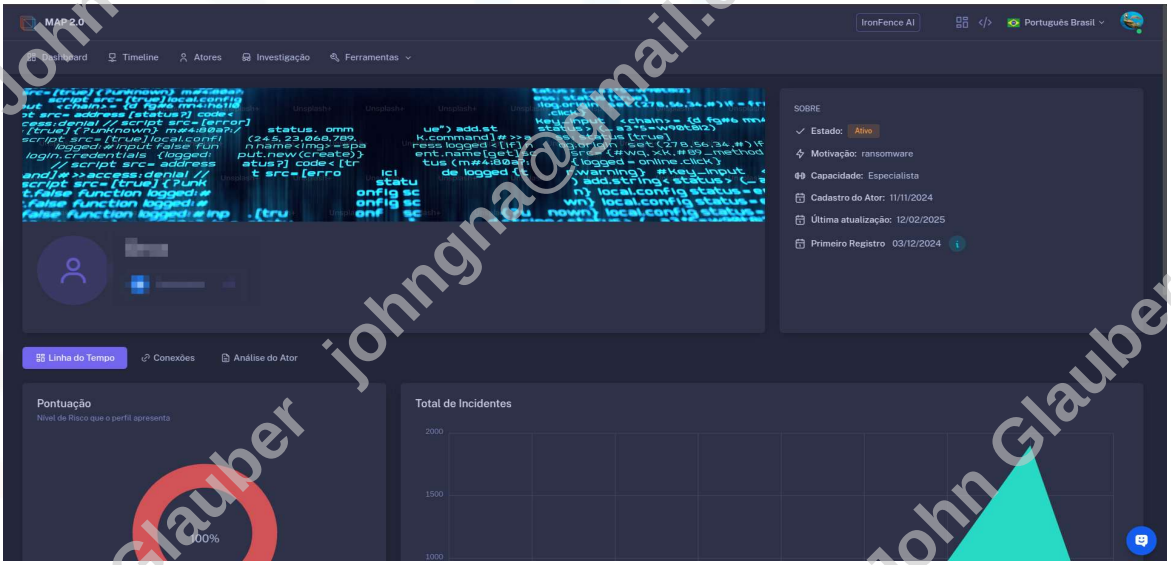
- **Modo Lista:** exibe os atores em formato de tabela, permitindo uma análise rápida e objetiva.
- **Modo Cards:** mostra cada ator em um card individual, destacando suas principais informações.



2. Perfil do Ator

Ao clicar no nome do ator, o sistema exibe uma página com detalhes completos, incluindo:

- **Estado:** se o ator está ativo ou inativo.
- **Motivação:** categoria do grupo (ex: **Ransomware**, **Hacktivismo**).
- **Capacidade:** nível de especialização do ator.
- **Histórico:** data do cadastro, última atualização e primeiro registro identificado.



3. Funcionalidades do Perfil

Dentro do perfil, há três opções principais:

- **Linha do Tempo:** exibe a progressão das atividades do ator ao longo do tempo.

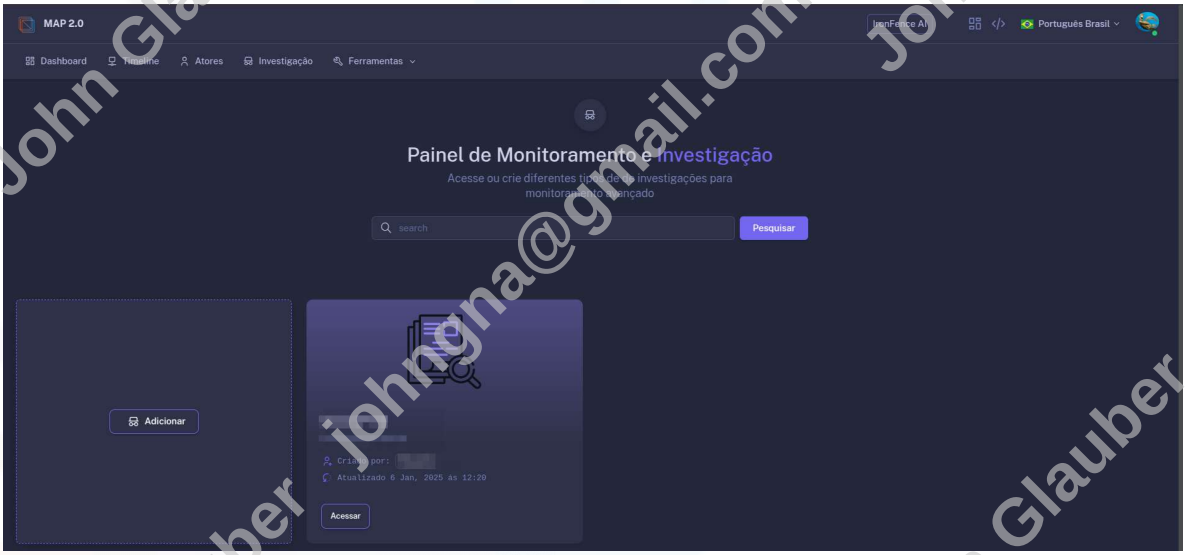
- **Conexões:** mostra possíveis relações do ator com outros grupos ou indivíduos.
- **Análise do Ator:** fornece uma visão aprofundada sobre suas ações e impacto.

INVESTIGAÇÃO

A tela de **Investigação** no MAP 2.0 permite a criação e gerenciamento de investigações detalhadas sobre ameaças cibernéticas. Nessa interface, os usuários podem definir critérios de busca avançados, segmentar incidentes e acompanhar o desenvolvimento de investigações específicas.

1. Painel de Investigação

- Apresenta uma visão geral das investigações criadas.
- Possui um campo de **pesquisa** para encontrar investigações existentes.
- O botão **"Adicionar"** permite a criação de uma nova investigação.



2. Criando uma Nova Investigação

Ao clicar em **"Adicionar"**, um modal de criação de investigação é exibido, permitindo a configuração de diferentes parâmetros:

I. **Descrição:** define o propósito da investigação.

II. **Alvo**: permite selecionar o alvo da investigação, como domínios, IPs ou sistemas autônomos.

III. **Ameaça:** filtra ameaças específicas relacionadas à investigação.

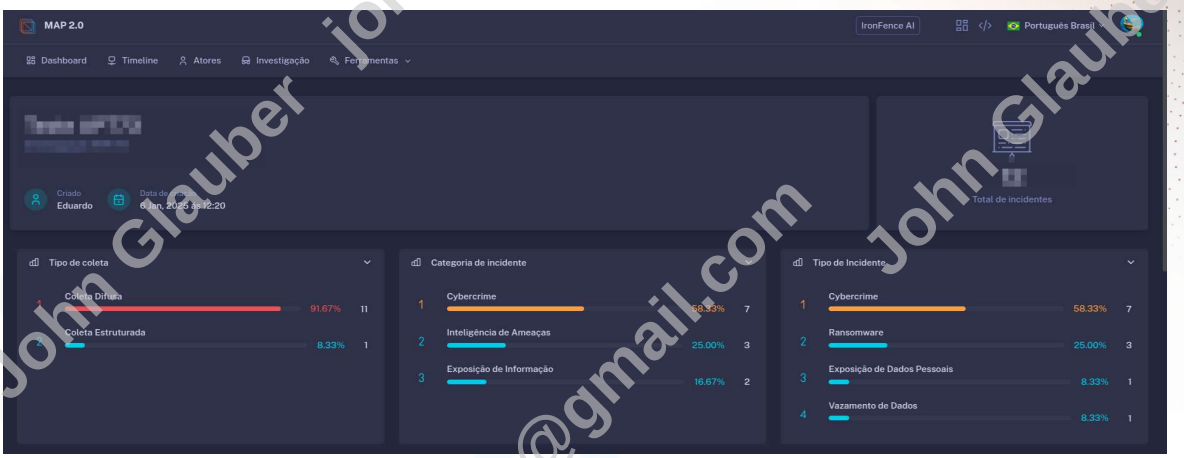
IV. **Origem:** especifica as fontes de dados, como listas negras, blogs e aplicativos de mensagens.

V. **Classificação:** define o tipo de incidente, categoria e coleta de dados.

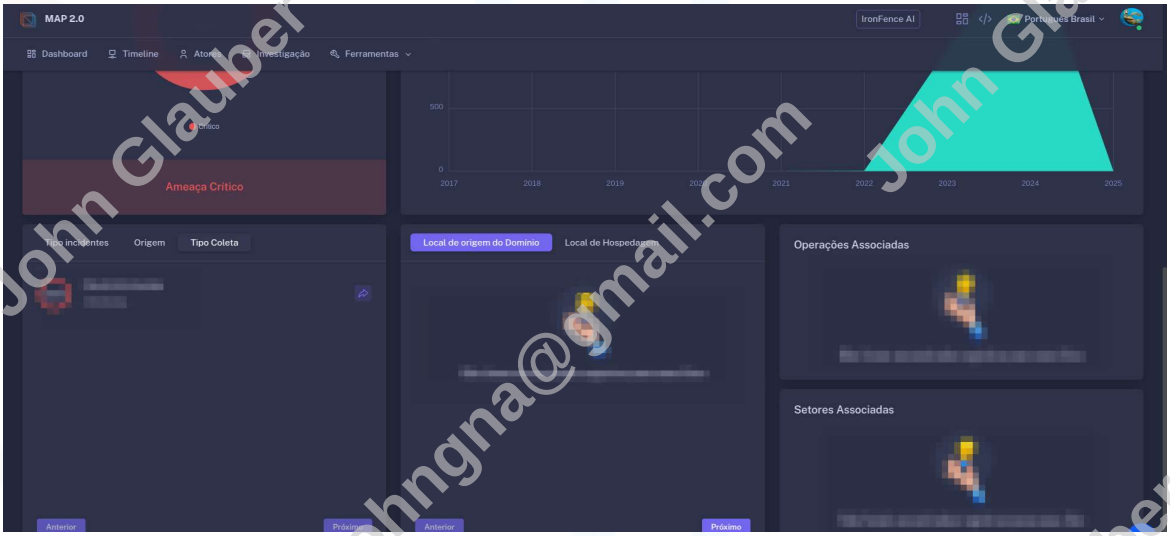
3. Tela de Investigação Ativa

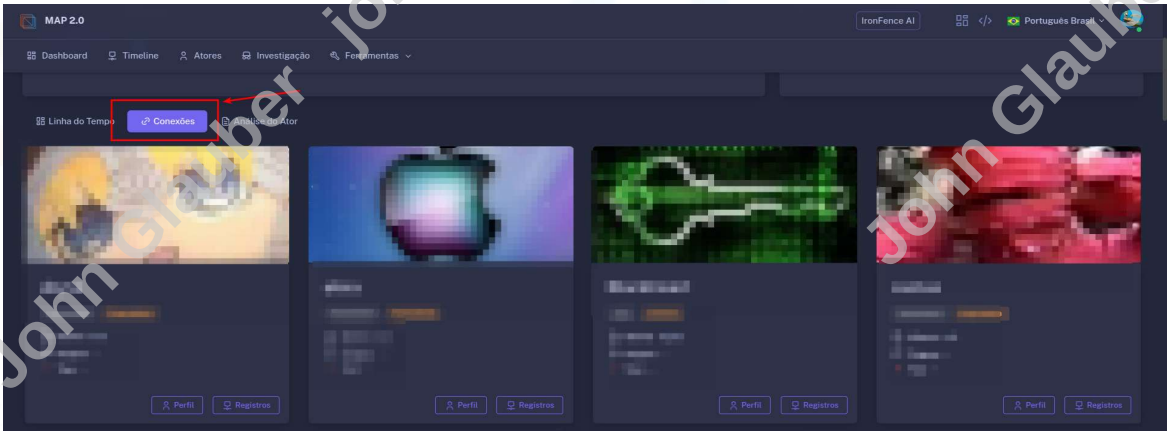
Após criada, a investigação exibe um painel detalhado com as seguintes informações:

- Criador e Data de Criação.
- Total de Incidentes coletados dentro dessa investigação.
- Distribuição por Tipo de Coleta, como Coleta Difusa ou Coleta Estruturada.
- Categorias de Incidentes, como Cybercrime, Inteligência de Ameaças, Exposição de Informações.
- Tipos de Incidentes, incluindo Ransomware, Vazamento de Dados e Exposição de Credenciais.



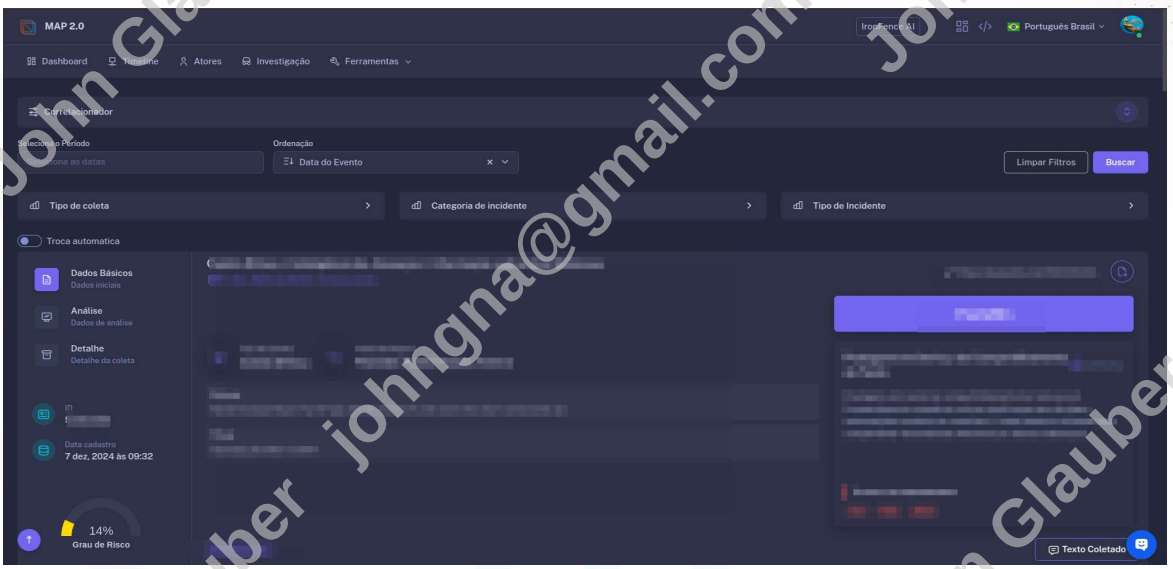
Essa seção do MAP 2.0 fornece ferramentas poderosas para a **análise e monitoramento de incidentes cibernéticos**, permitindo que os usuários personalizem suas investigações e acompanhem ameaças de forma detalhada.





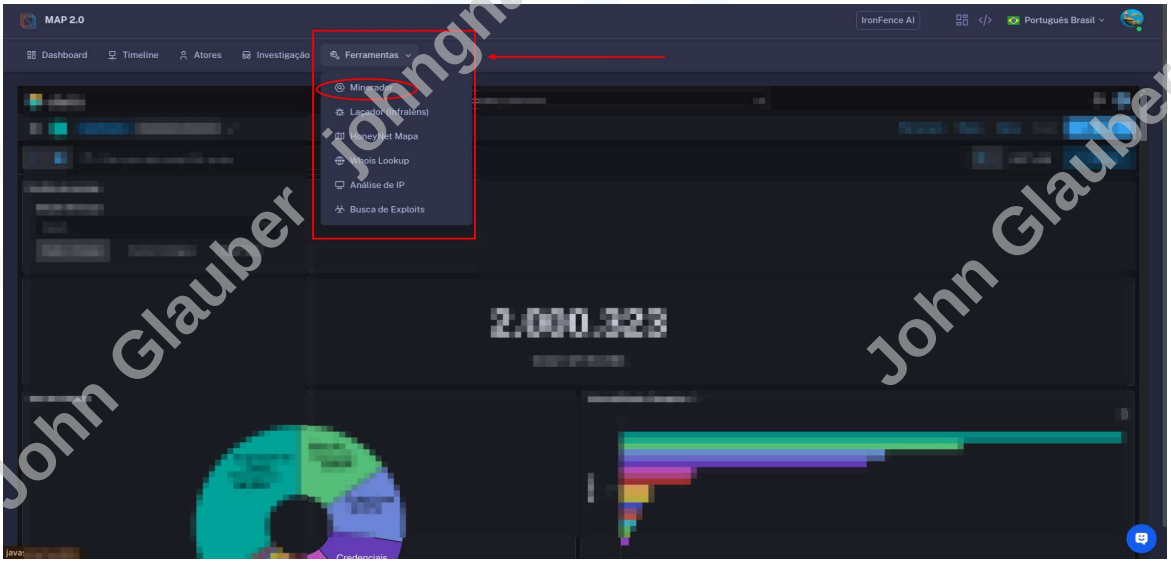
4. Registros do Ator

- O botão **"Registros"** redireciona diretamente para a **Timeline**, filtrando os incidentes associados ao ator selecionado.



Ferramentas - MAP 2.0

A seção **Ferramentas** do **MAP 2.0** disponibiliza um conjunto de utilitários para análise e investigação de ameaças, facilitando a detecção e resposta a incidentes. Cada ferramenta possui uma funcionalidade específica e uma interface própria.

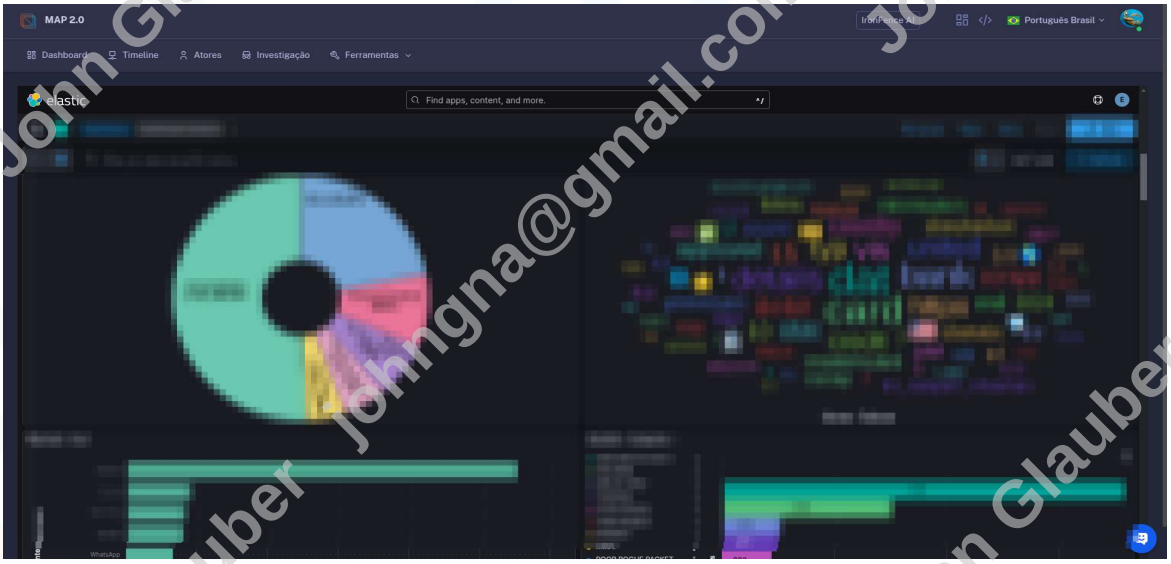


1. Minerador

O **Minerador** é um **dashboard do Elasticsearch** que centraliza grandes volumes de dados relacionados a ameaças cibernéticas. Ele permite filtrar, visualizar e analisar informações coletadas de diversas fontes.

Principais Funcionalidades:

- Contagem total de registros de incidentes.
- Análise de **tipos de incidentes**, como **exposição de credenciais, vazamento de dados e cybercrime**.
- **Distribuição de vulnerabilidades** e severidade dos riscos.
- **Origem dos dados**, incluindo principais fontes de coleta como Telegram, Pastebin e mercados clandestinos.
- **Tendências temporais** de atividades maliciosas.



2. Infralens

O Infralens é uma ferramenta de monitoramento de infraestrutura no MAP 2.0, focada na análise de endereços IP, domínios, servidores e vulnerabilidades associadas. Ele permite a identificação

de ameaças cibernéticas, análise de exposição de serviços e rastreamento de ativos de rede, utilizando um dashboard interativo no Elasticsearch.

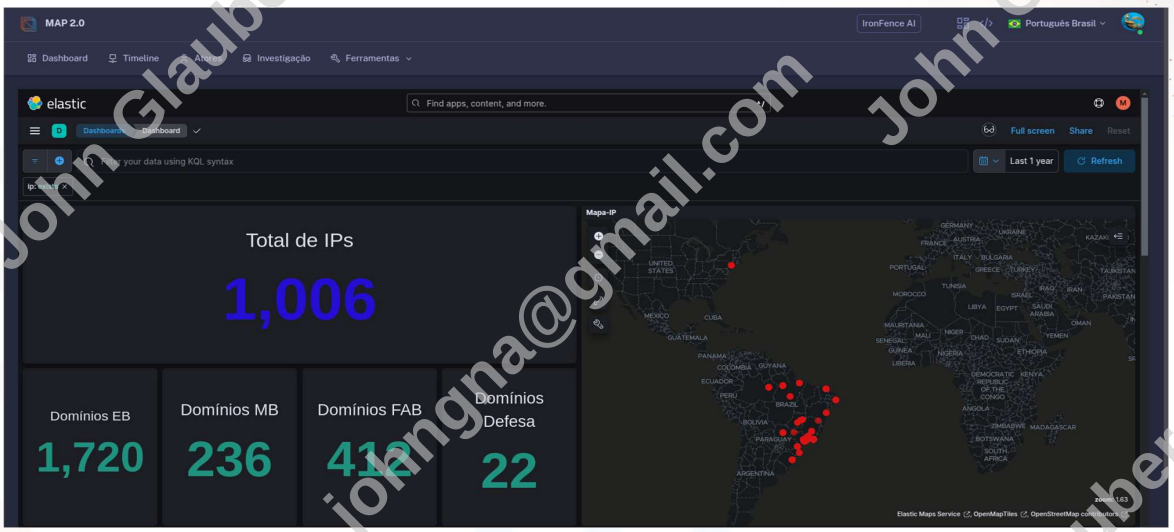
Funcionalidades:

- Total de IPs monitorados
- Classificação de domínios monitorados, segmentados em:
  - Domínios EB
  - Domínios MB
  - Domínios FAB
  - Domínios Defesa
- Mapa de geolocalização com distribuição dos IPs identificados
- Total de CVEs identificados nos ativos
- Classificação das vulnerabilidades por criticidade
- Tendência de detecção de CVEs ao longo do tempo
- Distribuição geográfica das infraestruturas monitoradas
- Servidores mais utilizados nas infraestruturas analisadas
- Portas abertas detectadas nos servidores
- IPs associados a CVEs críticos e alto risco
- Domínios com certificados HTTPS inválidos ou expirados

Finalidade:

- Monitoramento e investigação de ativos digitais
- Identificação de vulnerabilidades e riscos de exposição
- Análise detalhada de servidores e portas abertas
- Detecção de tendências de ataques cibernéticos
- Correlação de informações para mitigação de riscos

O Infralens permite a visualização detalhada dos ativos de rede, fornecendo dados estratégicos para a mitigação de riscos e a segurança cibernética.



3. HoneyNet Mapa

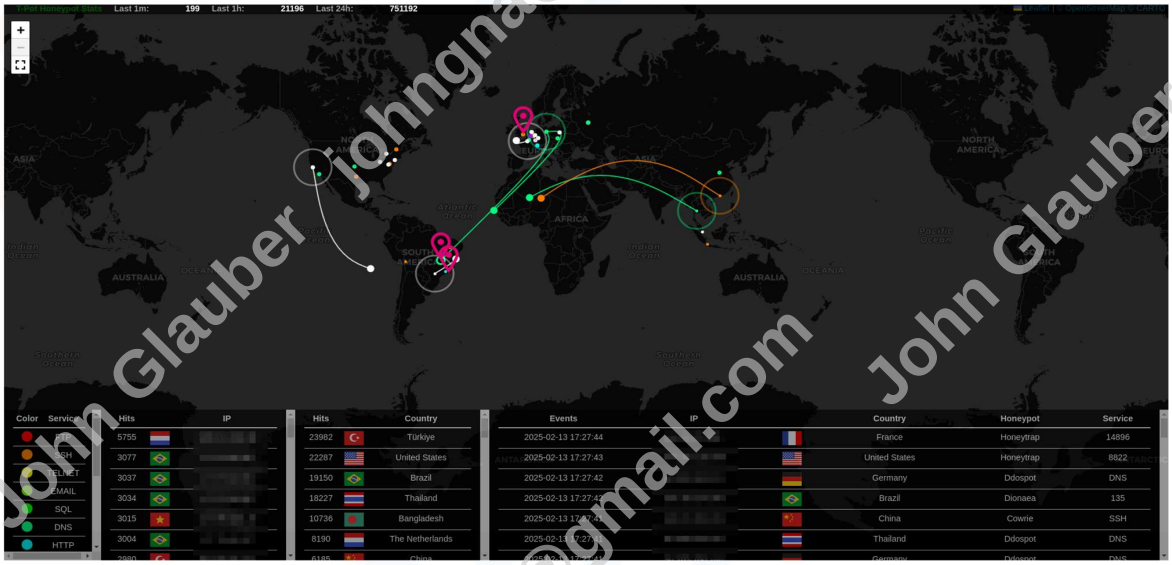
O HoneyNet Mapa é a nossa rede de honeypots integrada ao MAP 2.0, projetada para capturar, registrar e analisar ataques cibernéticos em tempo real ao redor do mundo. A ferramenta fornece um mapa interativo detalhado, permitindo o acompanhamento das tentativas de intrusão em diferentes regiões e a identificação das principais ameaças direcionadas a serviços específicos.

Funcionalidades:

- **Mapa Global Interativo:** exibe os ataques em tempo real, indicando origem, destino e vetores de ataque.
- **Registro Detalhado dos Eventos:** para cada tentativa de ataque, a ferramenta apresenta:
  - Endereço IP de origem
  - País do atacante
  - Tipo de honeypot detectado
  - Serviço explorado
  - Número de tentativas (hits)
  - Registro temporal do evento

- **Monitoramento em Tempo Real:** contadores exibem o número total de ataques nos últimos minutos, horas e 24 horas.
- **Ranking de Atacantes: l**ista dos IPs mais ativos, organizados por país e quantidade de tentativas de invasão.

A HoneyNet possibilita um entendimento aprofundado do cenário de ameaças, permitindo a análise de ataques direcionados em diversas partes do mundo e contribuindo para o fortalecimento das estratégias de segurança cibernética.

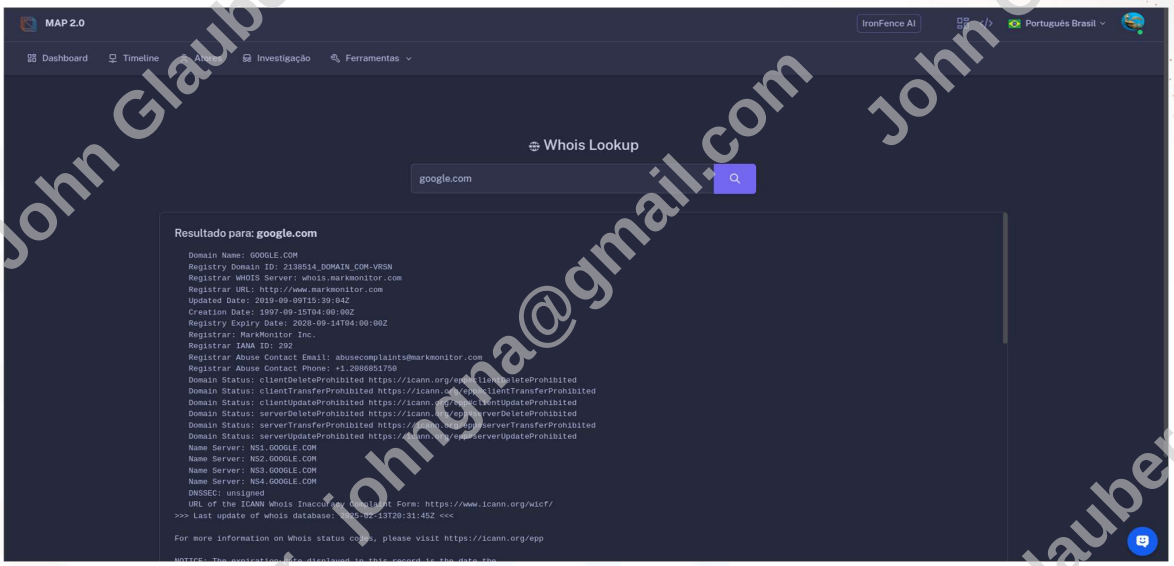


4. Whois Lookup

É uma ferramenta utilizada para realizar consultas detalhadas sobre a propriedade e status de um domínio na internet. A funcionalidade permite obter informações como o registrador do domínio, data de criação, data de expiração, servidores DNS, status de registro e contatos administrativos.

A partir da interface apresentada, o usuário pode inserir um domínio e visualizar os dados diretamente na plataforma. O resultado inclui informações sobre o provedor de registro, políticas de transferência e atualização do domínio, além de dados sobre a entidade responsável pelo gerenciamento do endereço consultado.

Essa ferramenta é essencial para investigações de segurança cibernética, permitindo verificar a autenticidade de domínios, identificar possíveis fraudes e mapear conexões entre sites suspeitos.



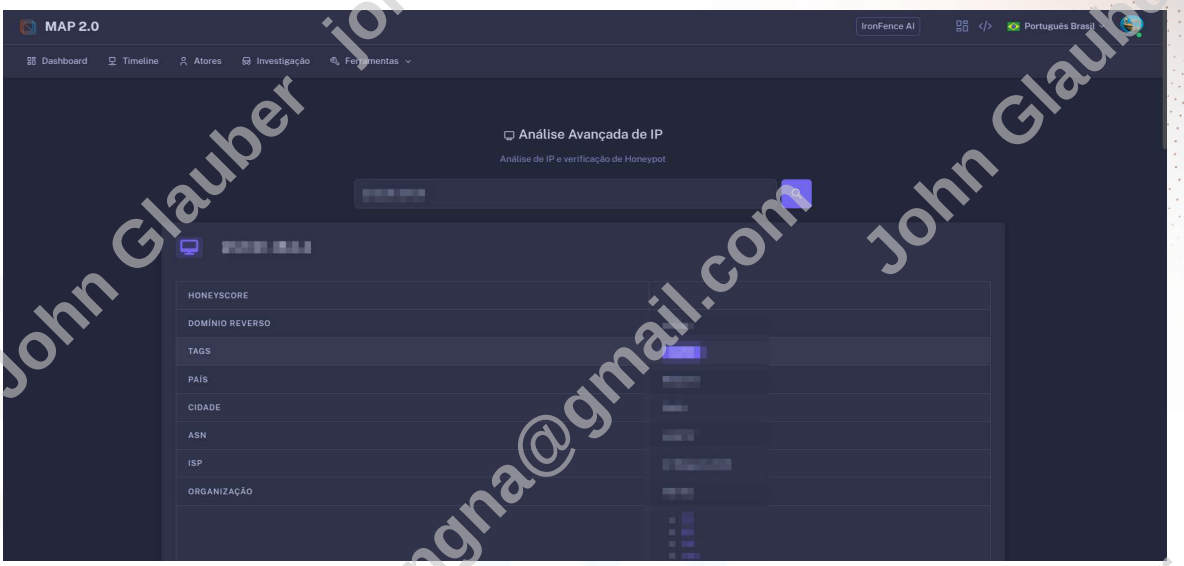
5. Análise de IP

A ferramenta Análise de IP do MAP 2.0 permite a investigação detalhada de endereços IP suspeitos, identificando origem, serviços expostos e vulnerabilidades.

Principais Funcionalidades:

- **Identificação do IP:** exibe ASN, ISP, organização e informações de domínio reverso.
- **Geolocalização:** apresenta país, cidade e coordenadas do IP.
- **Portas Abertas:** lista serviços ativos e protocolos em uso (HTTP, SSH, SMTP, etc.).
- **Detecção de Vulnerabilidades:** indica CVEs associadas e riscos de segurança.
- **HoneyScore:** avalia a possibilidade de o IP ser um honeypot.
- **Análises Adicionais:** detalha software, cabeçalhos HTTP e possíveis exploits.

A ferramenta auxilia na investigação de ameaças, monitoramento de IPs suspeitos e mitigação de riscos em redes corporativas.



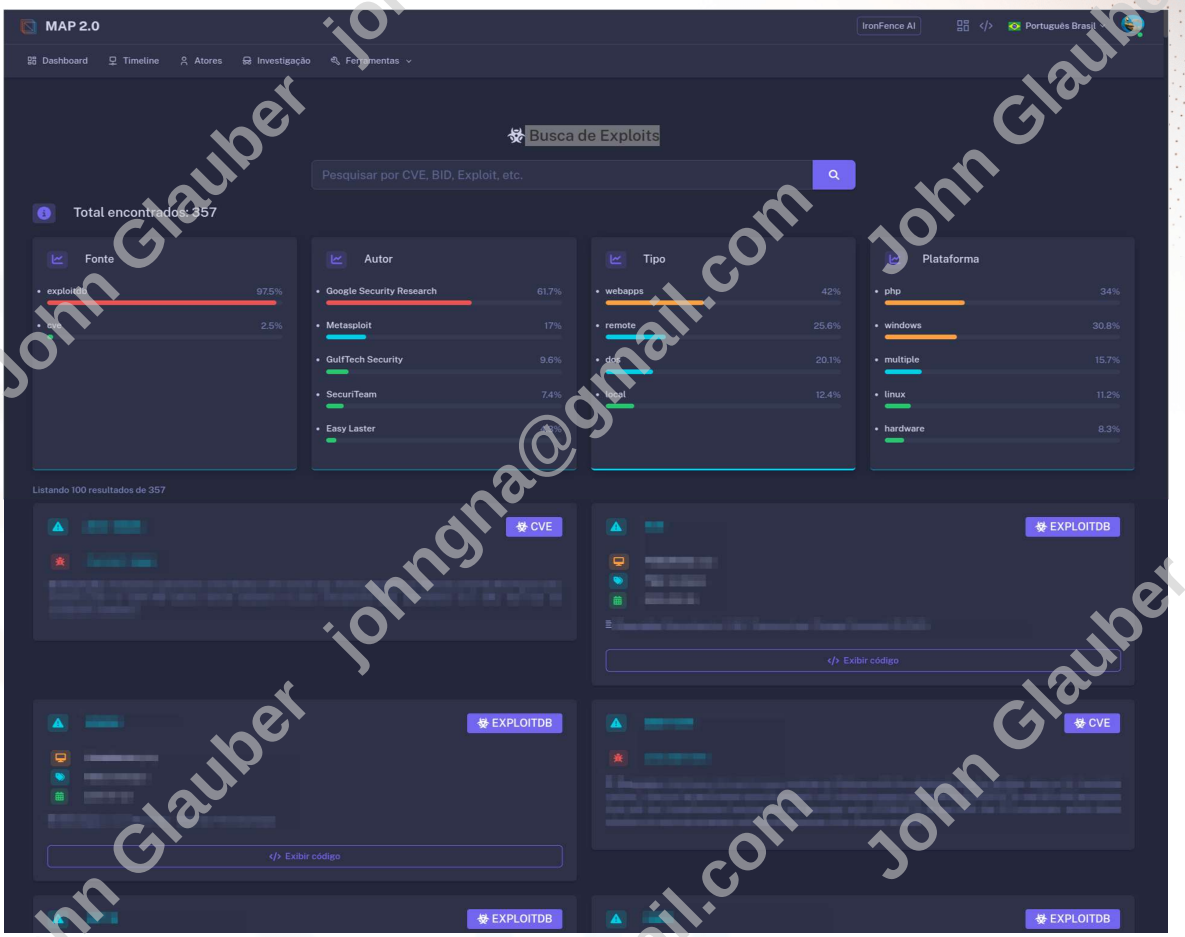
6. Busca de Exploits

A ferramenta **Busca de Exploits** permite a pesquisa detalhada de vulnerabilidades e exploits associados a sistemas, aplicações e serviços. O usuário pode realizar buscas por identificadores como **CVE, BID e Exploit**, retornando um conjunto de resultados organizados em diferentes categorias.

Principais Recursos:

- **Fonte dos Exploits:** indica a origem dos registros, destacando bases como ExploitDB e CVE.
- **Autor:** exibe os principais pesquisadores e equipes de segurança responsáveis pela descoberta dos exploits, como Google Security Research, Metasploit e GulfTech Security.
- **Tipo de Exploit:** classificação baseada na forma de exploração, incluindo webapps, remoto, DoS e local.
- **Plataforma:** segmentação dos exploits por ambiente afetado, abrangendo PHP, Windows, múltiplas plataformas, Linux e hardware.

A interface da ferramenta apresenta os resultados em formato estruturado, permitindo a rápida identificação das vulnerabilidades mais críticas e os métodos de exploração disponíveis.



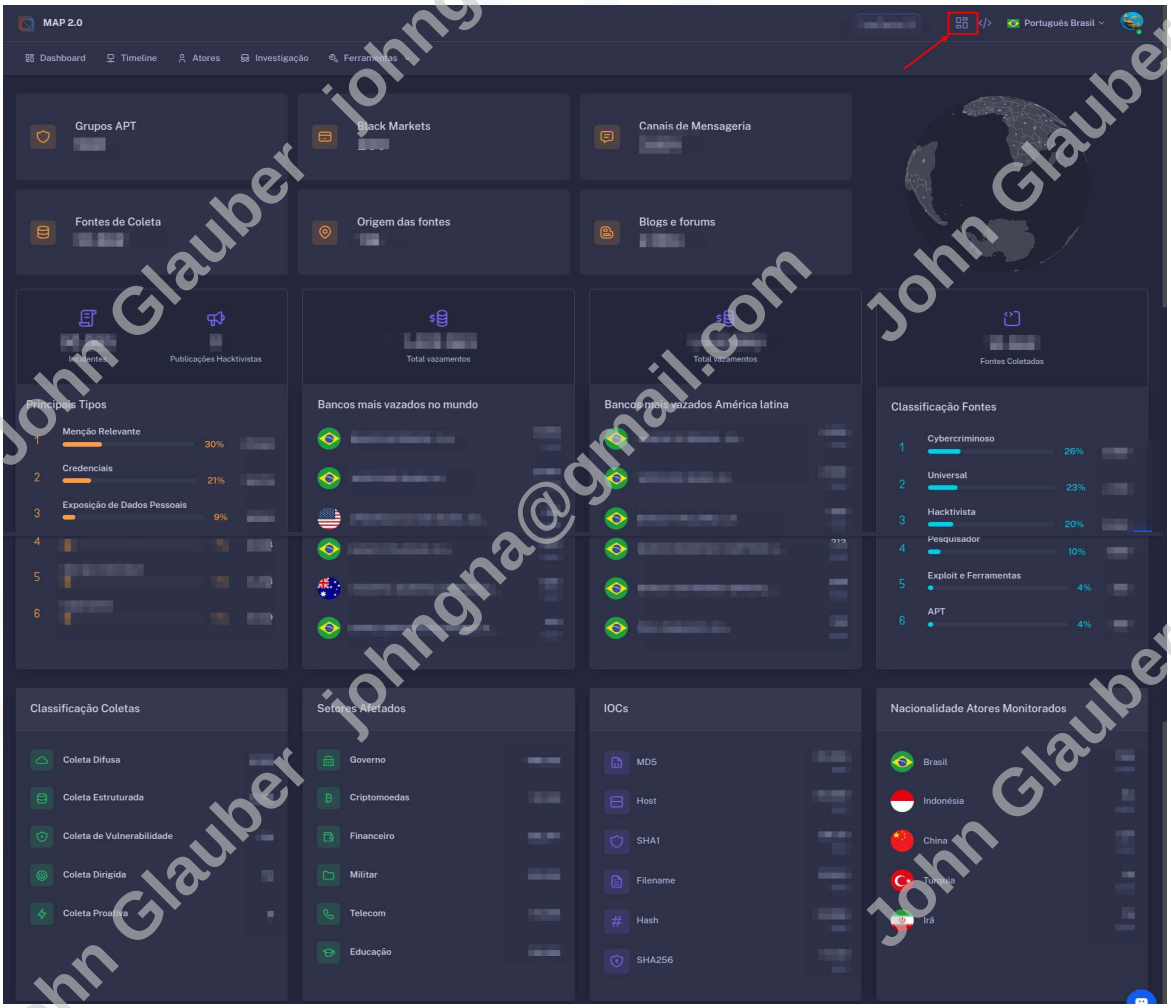
7. Panorama

A ferramenta Panorama do MAP 2.0 fornece uma visão abrangente das ameaças cibernéticas monitoradas, consolidando dados sobre grupos APT, vazamentos, incidentes e fontes de coleta. O painel destaca:

- **Grupos APT e Cybercrime:** identificação de atores maliciosos e sua atuação global.
- **Fontes de coleta:** monitoramento de canais como mercados negros, blogs, fóruns e redes de mensagens.
- **Incidentes e vazamentos:** contagem de eventos registrados, categorizados por credenciais expostas, menções relevantes e dados vazados.
- **Setores afetados:** áreas críticas impactadas, incluindo governo, financeiro, telecom e militar.

- **Classificação de coletas:** distribuição das informações coletadas entre coletas difusas, estruturadas e dirigidas.
- **IOC (Indicators of Compromise):** dados técnicos relevantes, como hashes, hosts e assinaturas de malware.
- **Nacionalidade dos atores monitorados:** estatísticas sobre a origem dos atores maliciosos.

O painel centraliza informações estratégicas para análise de ameaças, auxiliando na investigação e resposta a incidentes.



Caso tenha dúvidas ou precise de suporte técnico, entre em contato pelo e-mail **suporte@ironfence.ai** ou **pelo canal de suporte.**