Politécnico de Viseu FCCN Tecnologia para o Conhecimento FCT Fundação para a Ciência e a Tecnologia Jornadas 2022

IOCSNIFFER

Pedro Silva

02 de Junho de 2022

CERT RCTS

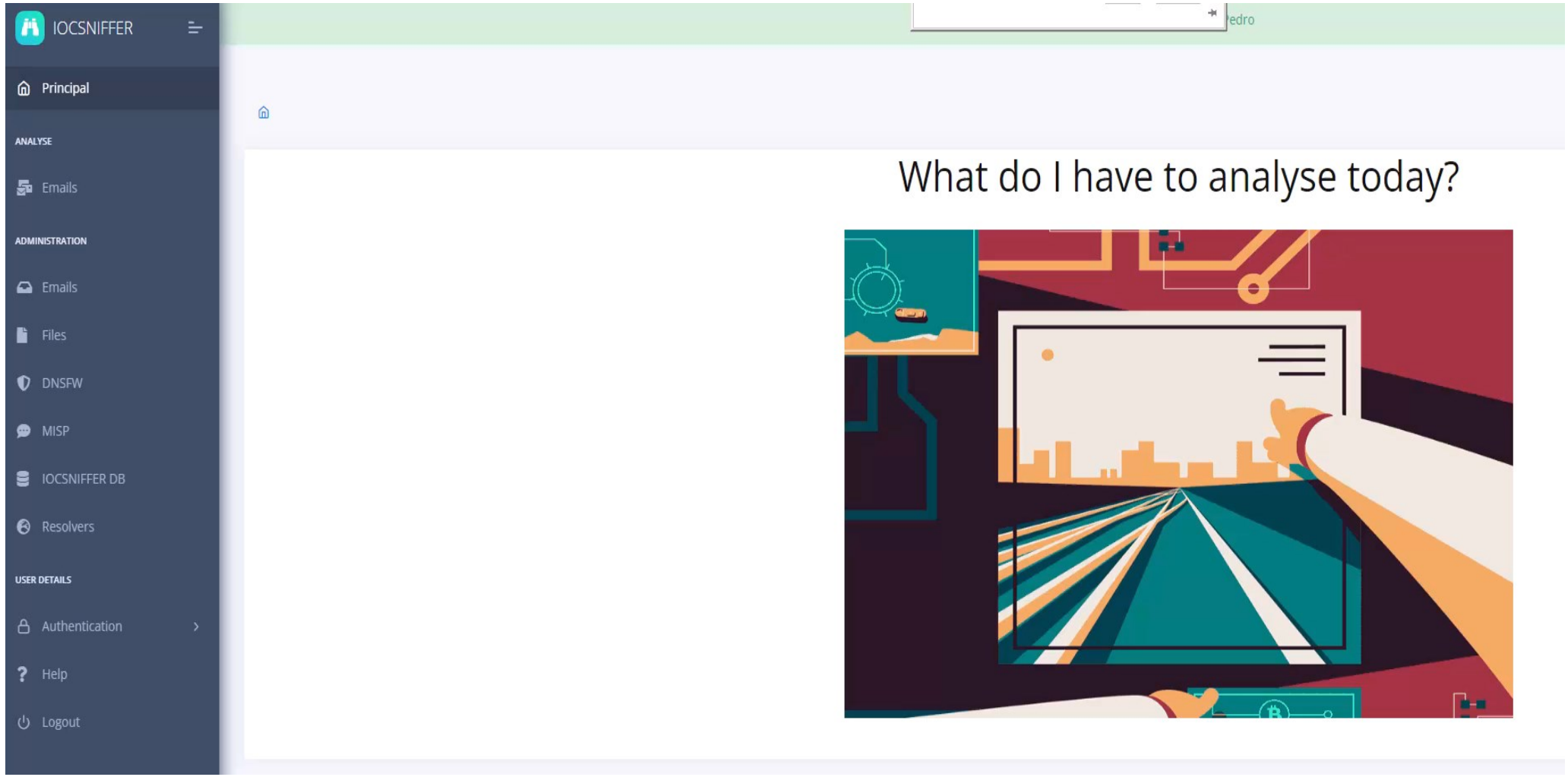
AGENDA

- Âmbito
- IOCsniffer
- Arquitectura
- Vídeo demonstrativo
- A desenvolver

ÂMBITO

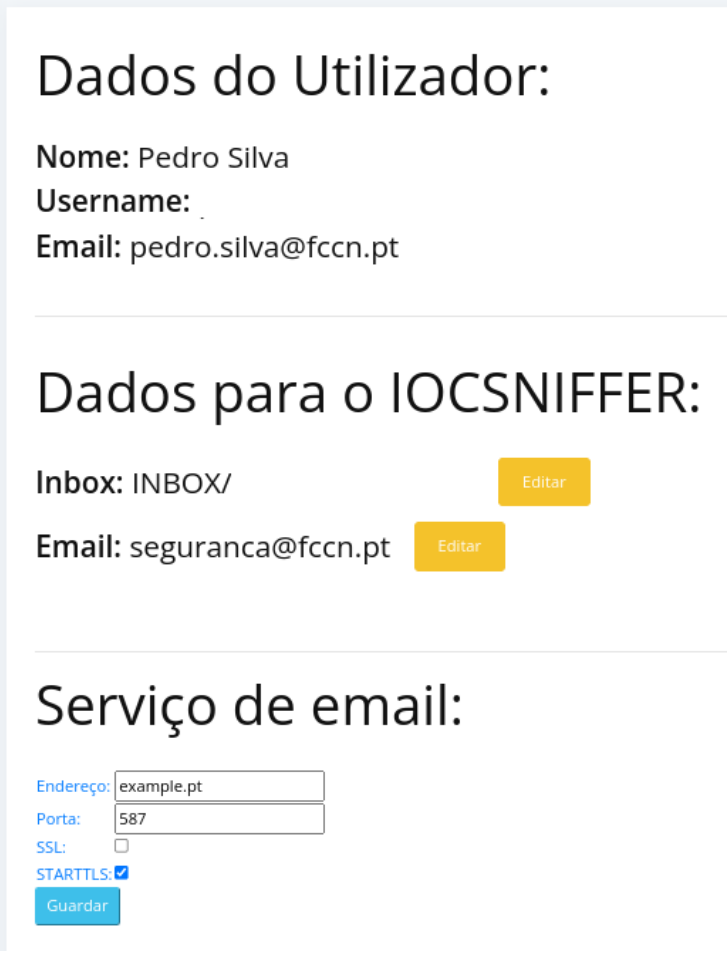
- **Porque foi criado?**
- **O que é?**
- **O que faz?**
- **Quem pode usar?**

IOCSNIFFER


IOCSNIFFER
Principal
ANALYSE
Emails
ADMINISTRATION
Emails
Files
DNSFW
MISP
IOCSNIFFER DB
Resolvers
USER DETAILS
Authentication
Help
Logout
What do I have to analyse today?

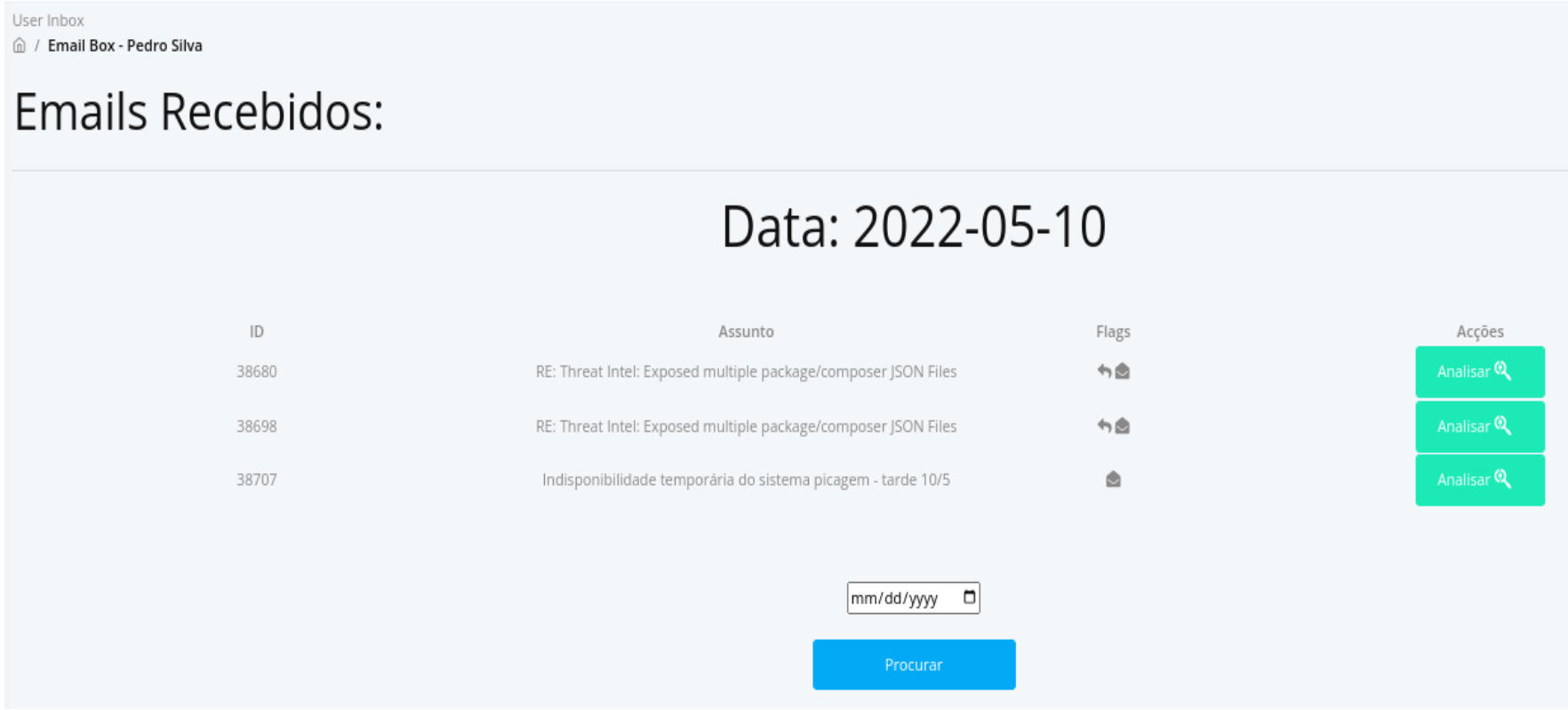
CONFIGURAÇÕES DE CADA UTILIZADOR

- **Dados do Utilizador**
- **Dados para o IOCsniffer**
- **Serviço de email**



ANALIZAR EMAILS DE UTILIZADORES 1/2

- **Analisar**
- **Procurar**

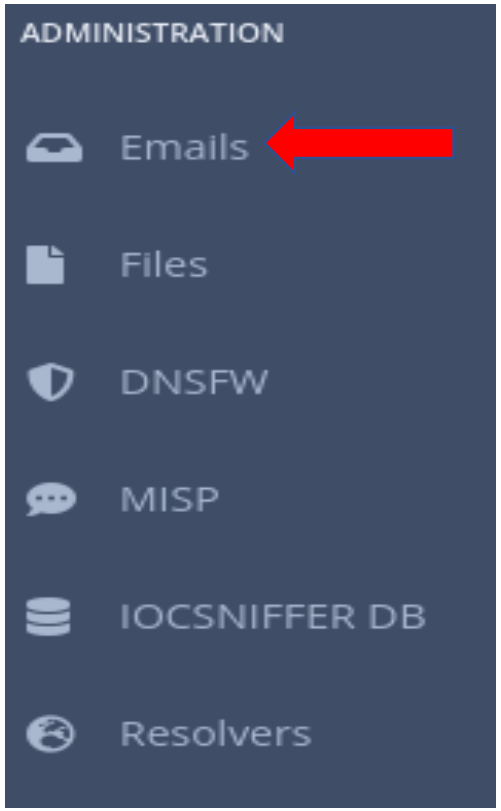


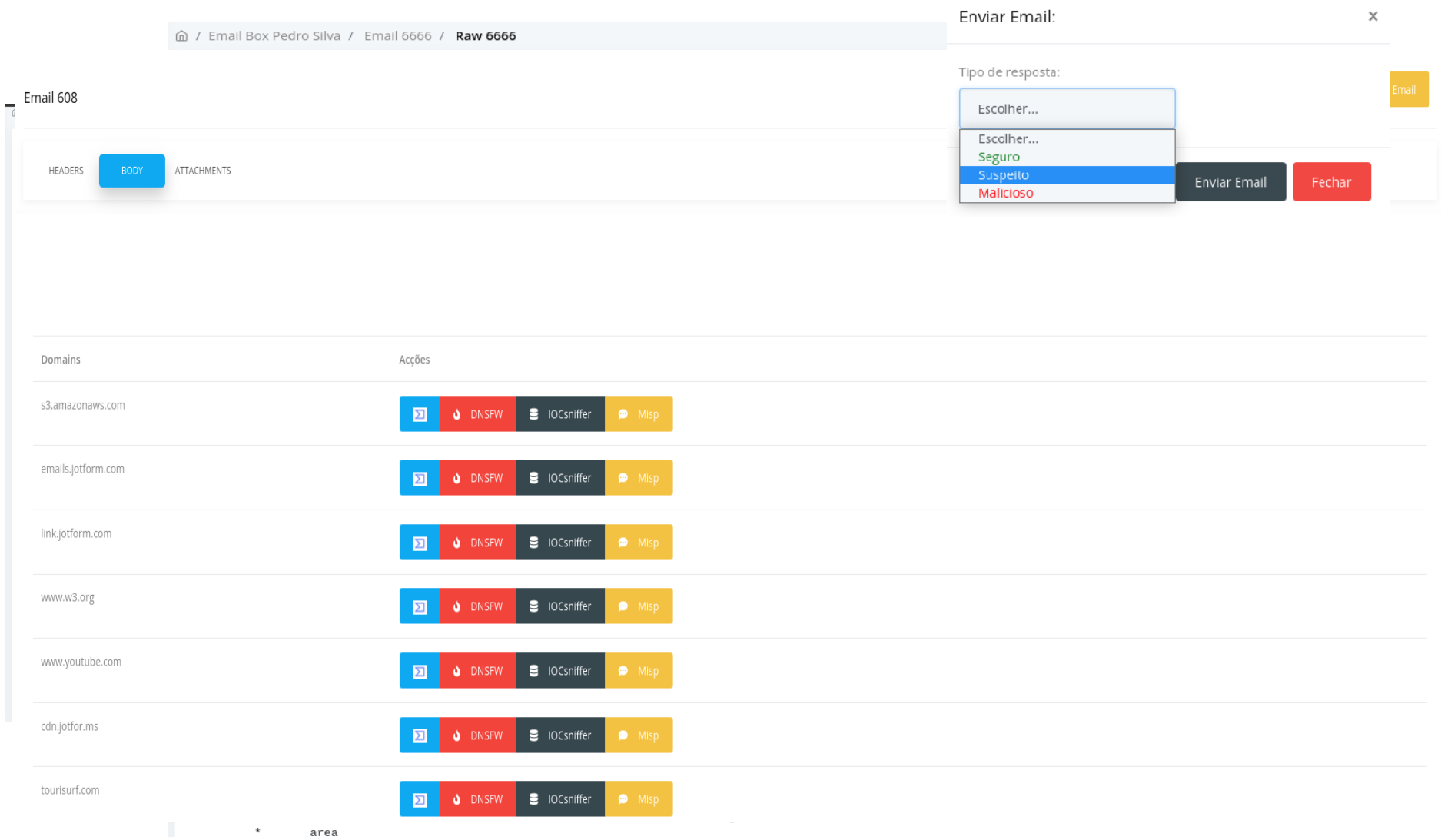
ANALIZAR EMAILS DE UTILIZADORES 2/2

- **Analisar 1 email…**

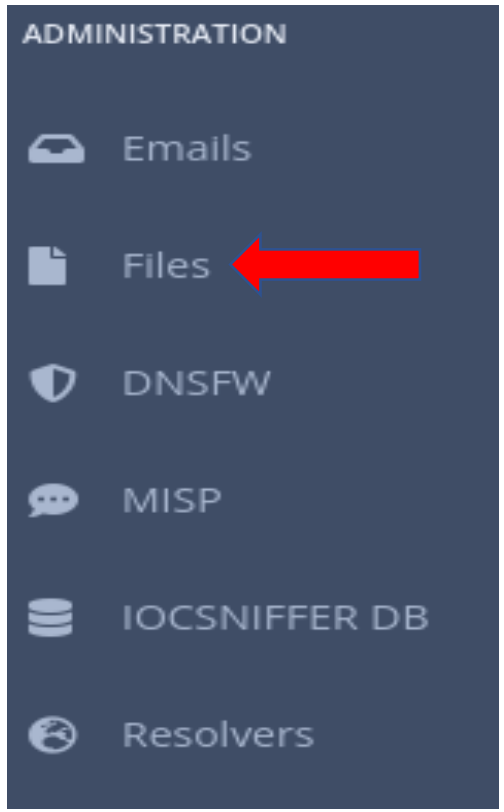
- **Aparentemente Seguro**
- **Suspeito**
- **Malicioso**

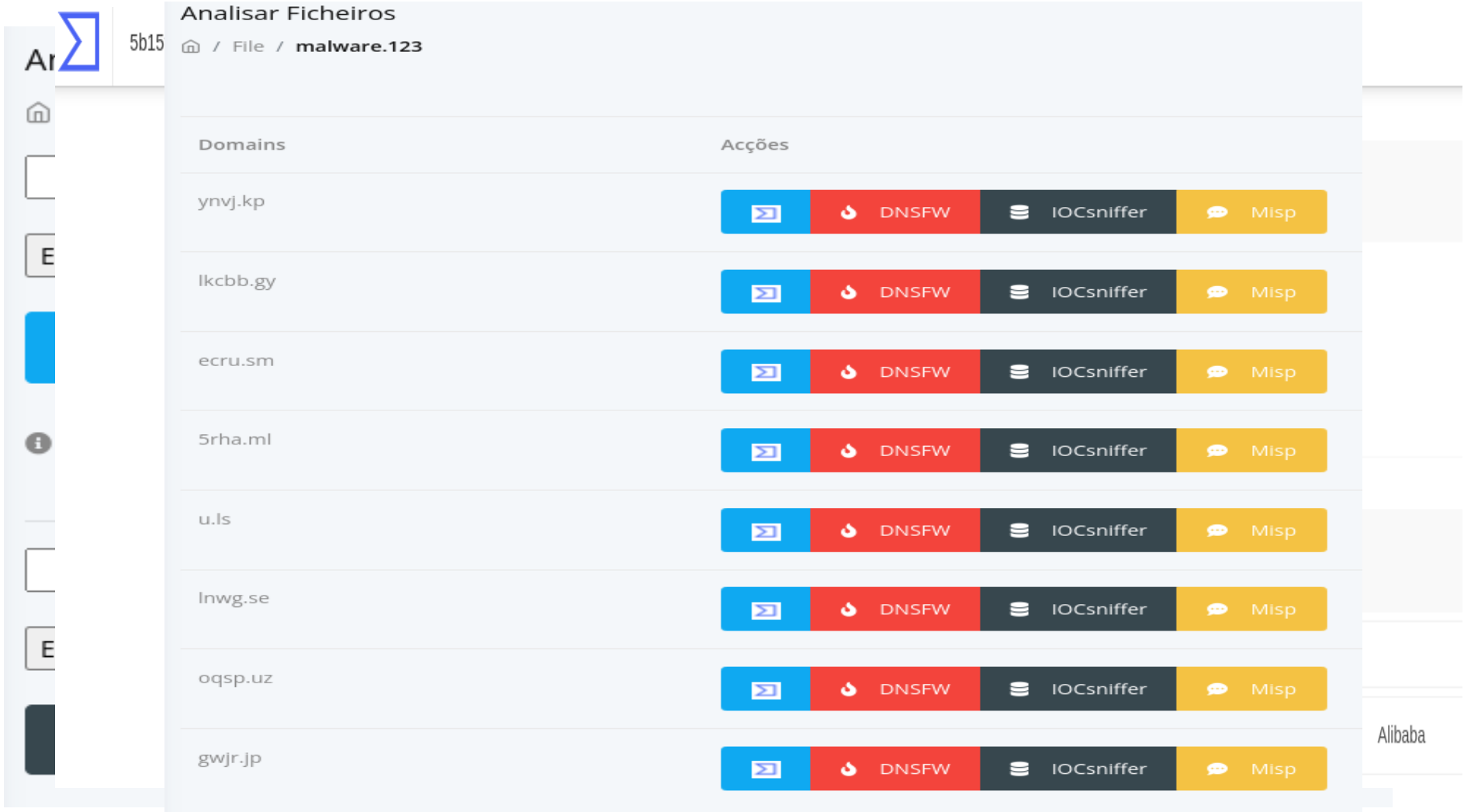
Analistas EMAILS



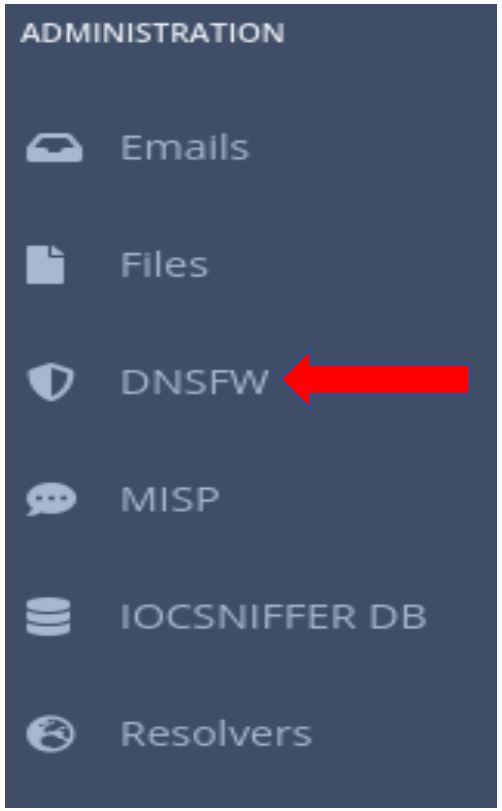


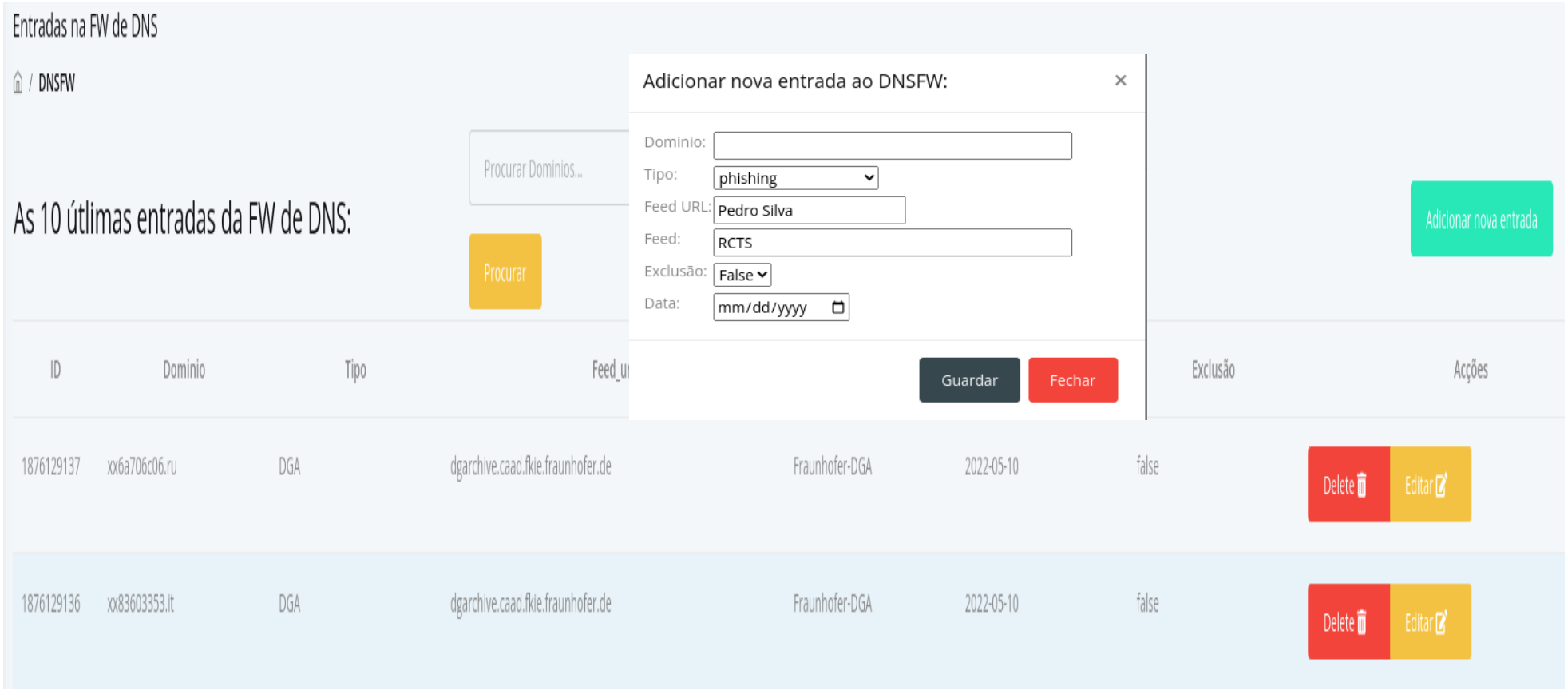
Analistas FILES



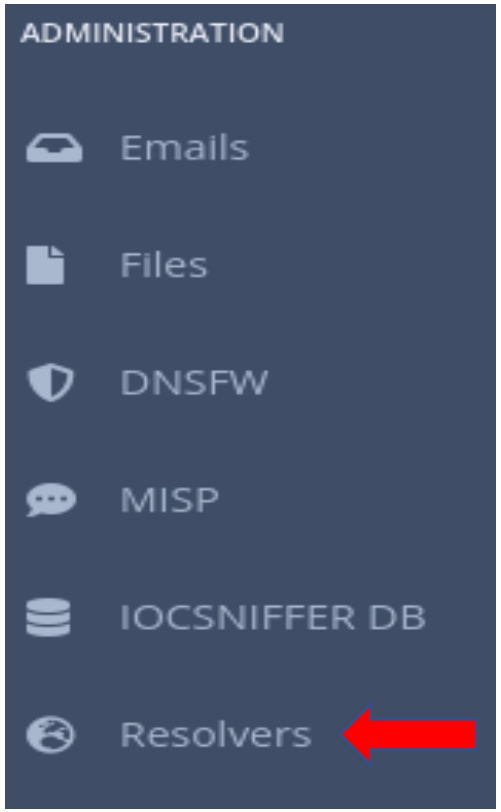


Analistas DNSFW





Analistas Resolvers



Enviar entradas da DNSFW para os resolvers

/ Resolvers

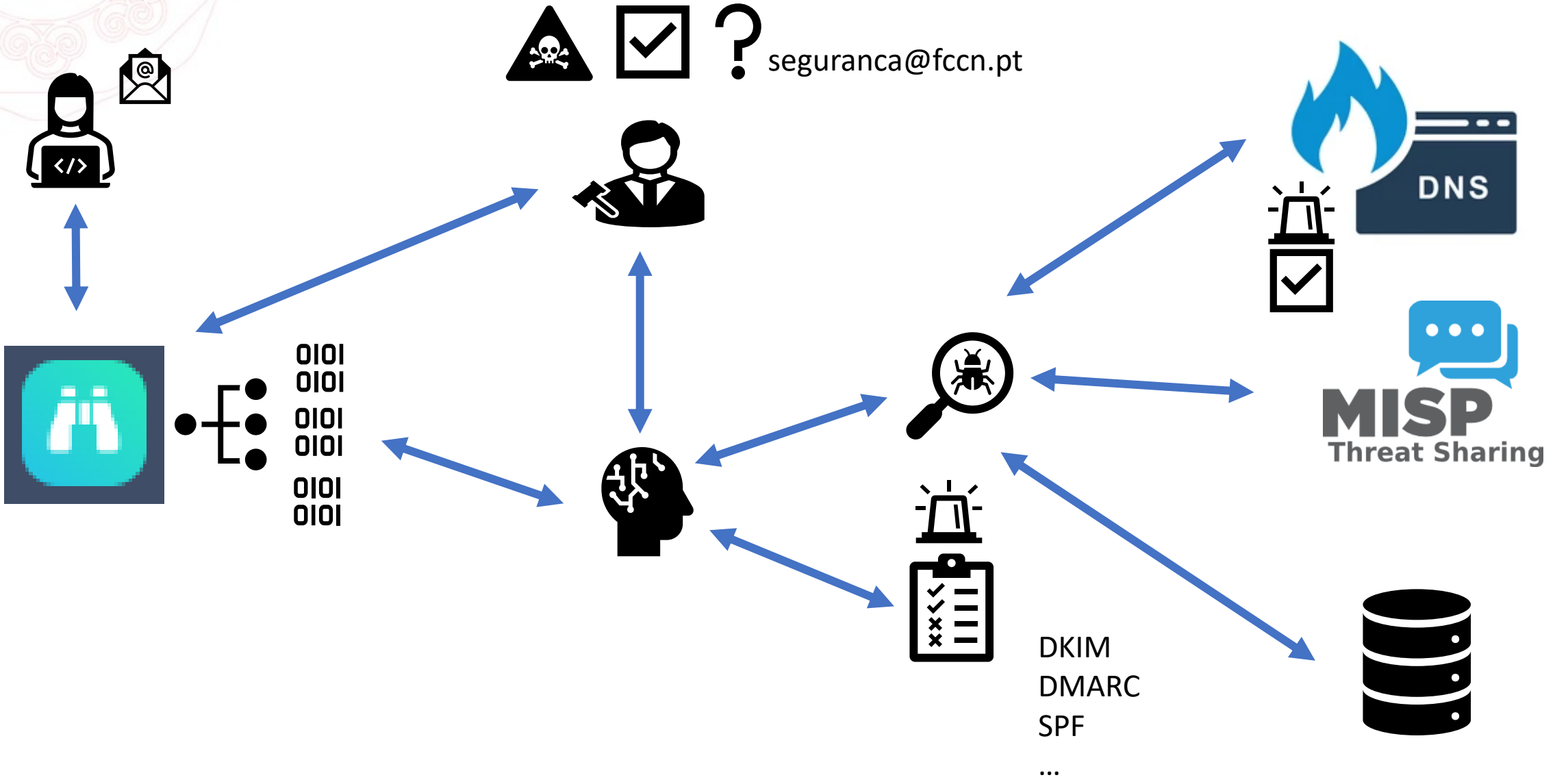
Enviar entradas da DNSFW para os resolvers

/ Resolvers

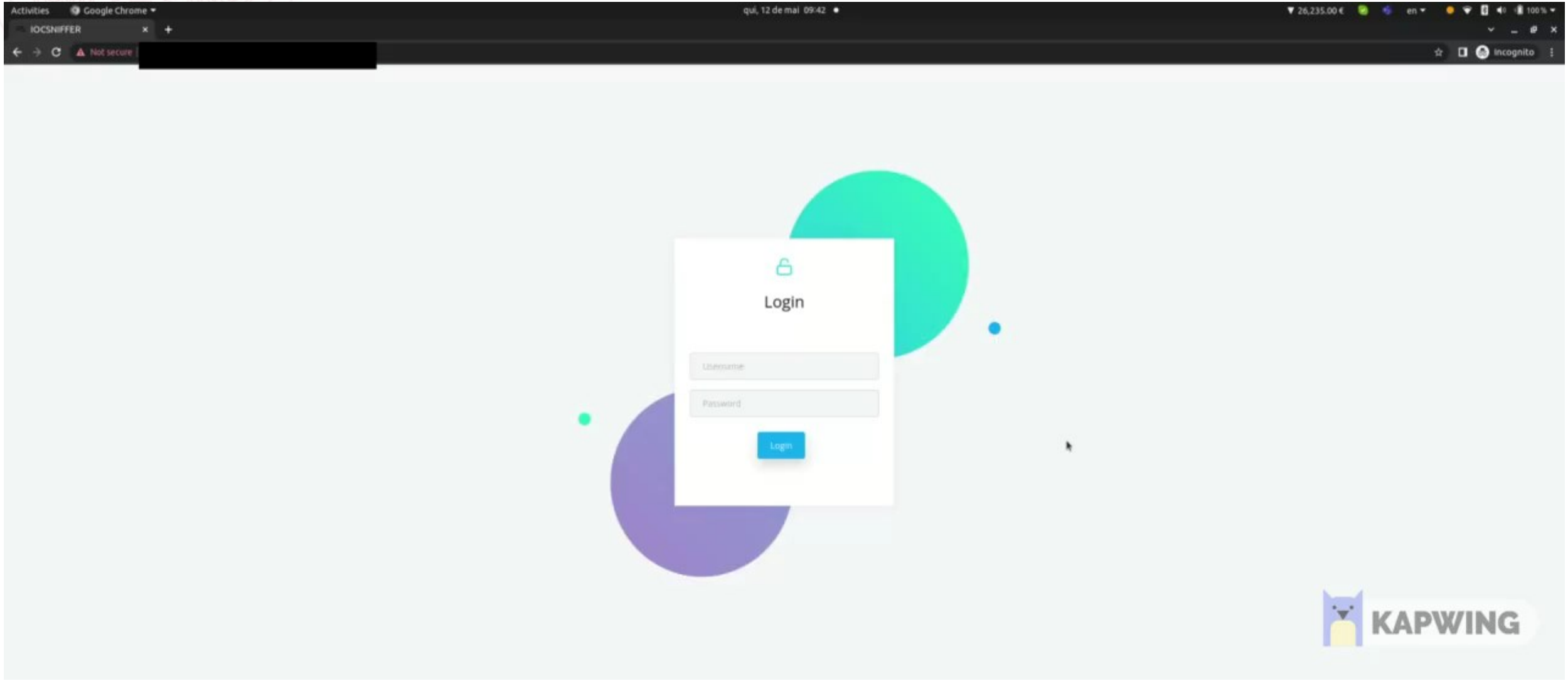
Push para os resolvers de DNS

ID	Data	Estado	Username
4	2022-03-15 15:46:52.217490	Error	
5	2022-03-15 15:51:12.230912	Done	
6	2022-03-22 17:33:26.128694	Error	
7	2022-03-22 17:33:35.340998	Error	
8	2022-03-22 17:33:51.631687	Error	
9	2022-03-22 17:34:07.151177	Error	
10	2022-03-22 17:36:41.543507	Error	
11	2022-03-22 17:38:16.126566	Error	
12	2022-03-23 10:11:25.841714	Done	
13	2022-03-25 12:22:48.474212	Done	
14	2022-04-13 08:17:03.466827	Done	
15	2022-04-13 09:15:47.919094	Done	
16	2022-04-20 13:38:02.985103	Done	

Arquitectura



Vídeo Demonstrativo



A DESENVOLVER

- Autenticação Federada
- Configurar Serviço de Email
- Adicionar mais lógica
- Multiprocessing
- Melhorar a página de ajuda
- Análise de ficheiros/anexos
- Estatísticas

Obrigado!