RNP

Educação, Pesquisa
e Inovação em Rede

Você realmente conhece sua superfície de ataque?

ARGUS – Exposição real e visibilidade contínua com IVRE

cais Inteligência em Cibersegurança

TLP:CLEAR

Superfície de ataque – Exposição e Visibilidade com ARGUS (IVRE)

- **Superfície real de ataque**
  - Onde o inventário estático falha
- **IVRE**
  - Arquitetura e recursos
- **Análise**
  - Coleta ativa, passiva e indexação
- **Casos de uso**
  - Blueteam, SOC, CSIRT e CTI
- **Projeto ARGUS**
  - Experiência da RNP

(landim㉿cais-rnp)-[~]
$ whoami
André Ricardo Landim

- ***Antes de tudo, sou filho, marido e pai*** *— o que, por si só, já exige habilidades avançadas de negociação, resposta a incidentes e gestão de crises em tempo real;*

- *Também* ***trabalho com Tecnologia da Informação há mais de <ANTIGÃO> anos e os últimos <REDACTED> anos foram dedicados à Segurança*** *da Informação;*

- *Já* ***atuei em áreas como segurança de infraestrutura, Red e Blue Team, DFIR*** *e análise de malwares;*

- ***Atualmente, atuo como Especialista em Segurança no CAIS, equipe de Cibersegurança e Inteligência da RNP*** *(Rede Nacional de Ensino e Pesquisa) e que por acaso também agrega o CSIRT e o SOC;*

- *No fim das contas,* ***sigo tentando equilibrar tecnologia, segurança, família e café****, nem sempre nessa ordem;*

- *LinkedIn: https://www.linkedin.com/in/andrelandim/*

TLP:CLEAR

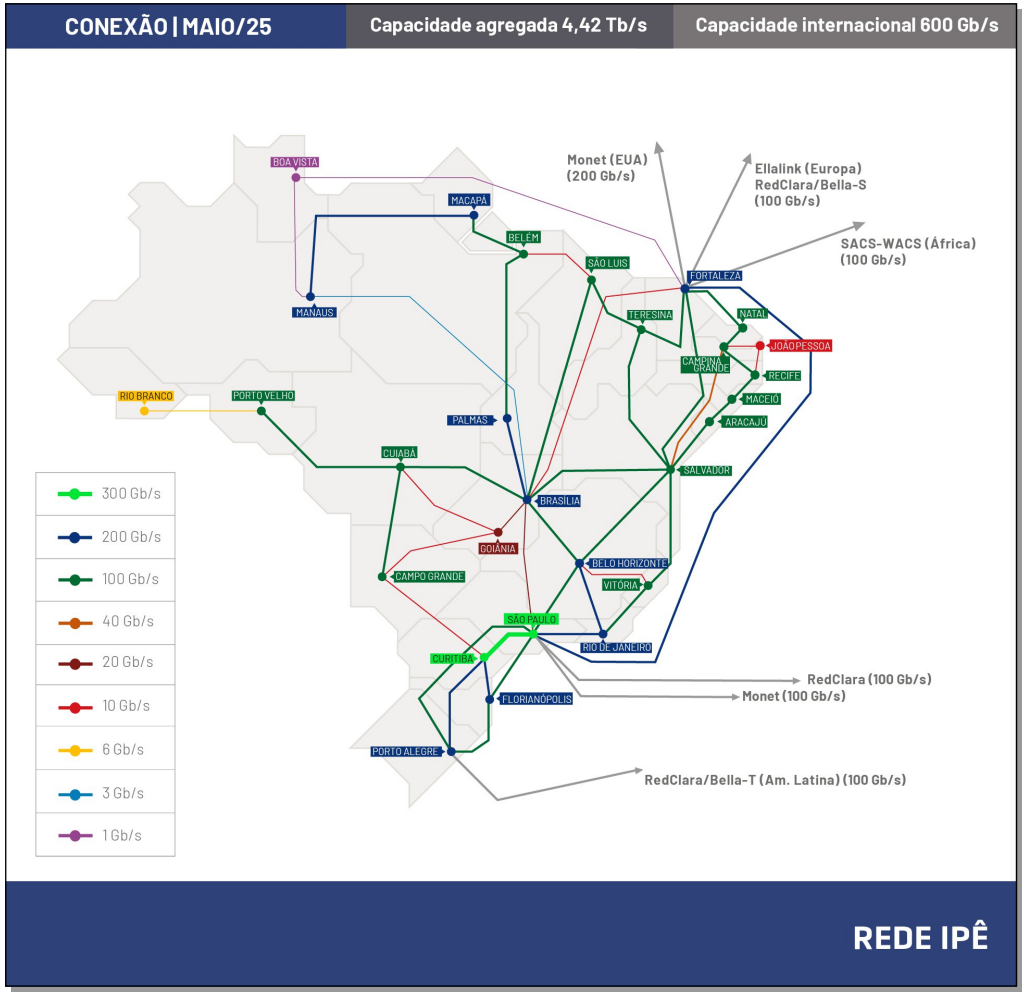
Sobre a RNP...

Conectamos universidades e instituições de ensino, pesquisa e inovação com internet e serviços seguros em uma comunidade, o Sistema RNP.

Nesse ambiente, trabalhamos em conjunto com alunos, professores e pesquisadores para desenvolver novas tecnologias com foco em inovação contínua.

É por meio dessa rede acadêmica que a ciência brasileira compartilha conhecimento e colabora entre si e com parceiros em todo o mundo.

Somos uma organização social vinculada ao governo federal e apoiamos políticas públicas de ensino e pesquisa.



TLP:CLEAR

Sobre a CAIS...

Há 26 anos, o CAIS-RNP garante a segurança em centenas de instituições de educação e pesquisa brasileiras.

A área de inteligência em cibersegurança da RNP desenvolve ações preventivas, educativas e corretivas em incidentes e ameaças na rede acadêmica, que enfrenta diariamente os desafios ligados ao aumento da complexidade de ameaças cibernéticas.

Inventário != Superfície de ataque

CMDB / Inventário

- Ativos
- Responsáveis
- Finalidade
- Criticidade
- Ciclo de vida

Superfície observável

- “Ativos vivos”
- Portas e serviços
- Certificados
- Ativos desatualizados

Diferença prática

A exposição — a superfície observável — é onde reside grande parte do risco operacional.

O “dilema” da superfície observável...

Muitos sinais, muitos dados e muitas perguntas.

O **desafio não é apenas coletar informações. O desafio é**:

- saber o que está exposto
- o que mudou
- o que importa
- o que deve ser priorizado

Com visibilidade contínua, temos o fluxo básico...

1. **Coleta recorrente**
2. **Consulta de ativos na base de dados**
3. **Histórico comparativo**
   - Novo
   - Removido
   - Persistente
4. **Priorização**
   - Crítica
   - Alta
   - Média
   - Validação
   - Tratamento
   - Notificação
   - Monitoramento

TLP:CLEAR

Com visibilidade contínua, mudamos algumas coisas...

Mudança de cenário:

- *De: "Eu acho que sim..."*
- *Para: "Sim, e essa é a situação..."*

Redução de:

- incertezas
- tempo de triagem

Ações orientadas (priorização):

- evidências técnicas
- criticidade

TLP:CLEAR

O que é o IVRE...

- ***IVRE is an open-source framework for network recon. It relies on open-source well-known tools*** *(Nmap, Masscan, ZGrab2, ZDNS and Zeek (Bro))* ***to gather data*** *(network intelligence), stores it in a database (MongoDB is the recommended backend),* ***and provides tools to analyze it****.*
- ***It includes a Web interface aimed at analyzing Nmap scan results*** *(since it relies on a database, it can be much more efficient with huge scans than a tool like Zenmap, the Nmap GUI, for example).*
- ***IVRE*** *means "Instrument de veille sur les réseaux extérieurs", and* ***is French for DRUNK****, "Dynamic Recon of Unknown NetworKs".*
- ***It's free software****, the code is on GitHub and the documentation on Read the Docs.* ***Enjoy!***

https://ivre.rocks/

TLP:CLEAR

O que podemos fazer...

Coleta ativa / Enriquecimento

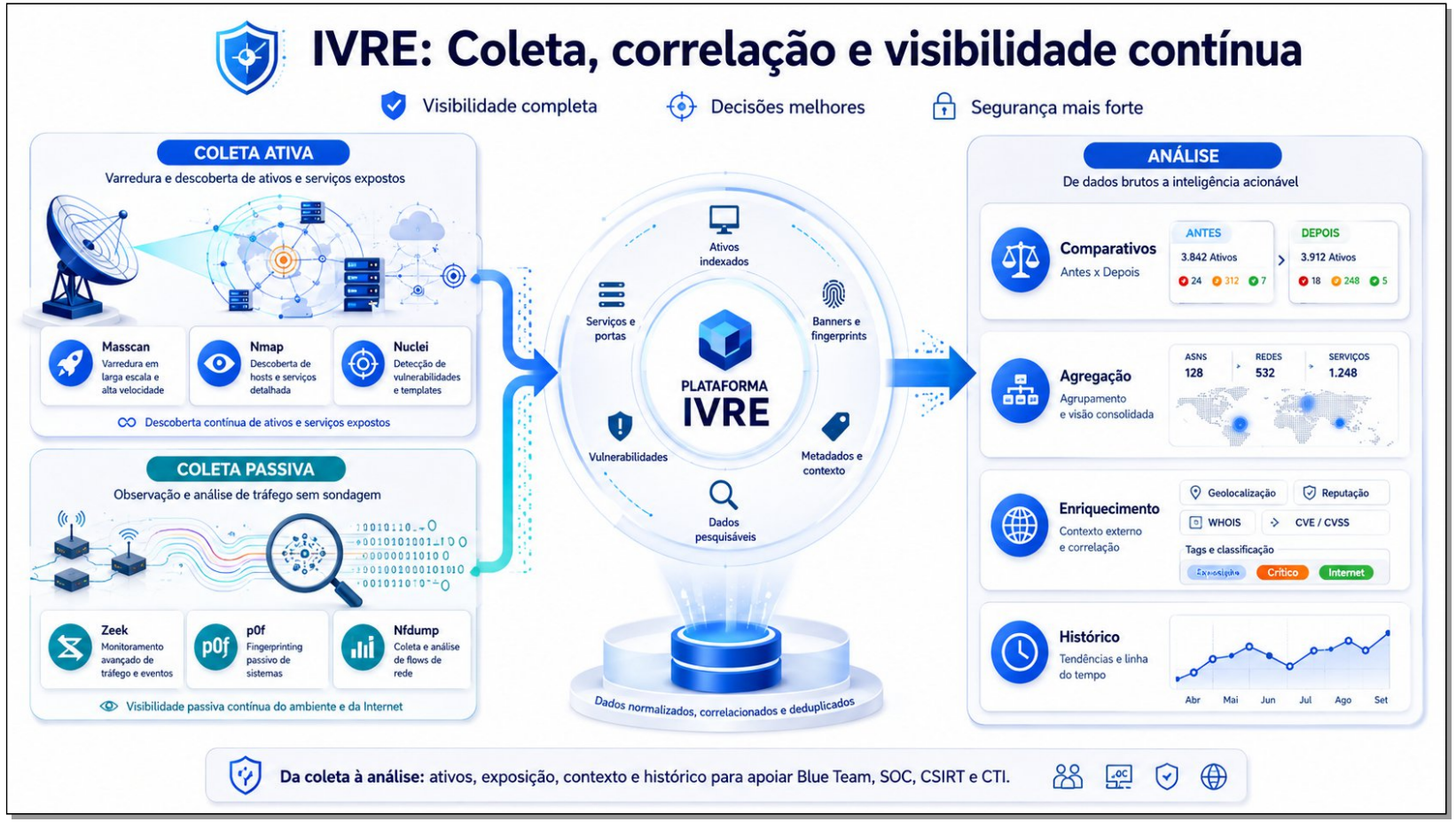
- *Masscan*
- *NMAP*
- *Nuclei*

Coleta passiva

- *Zeek*
- *p0f*
- *Nfdump*

Análise

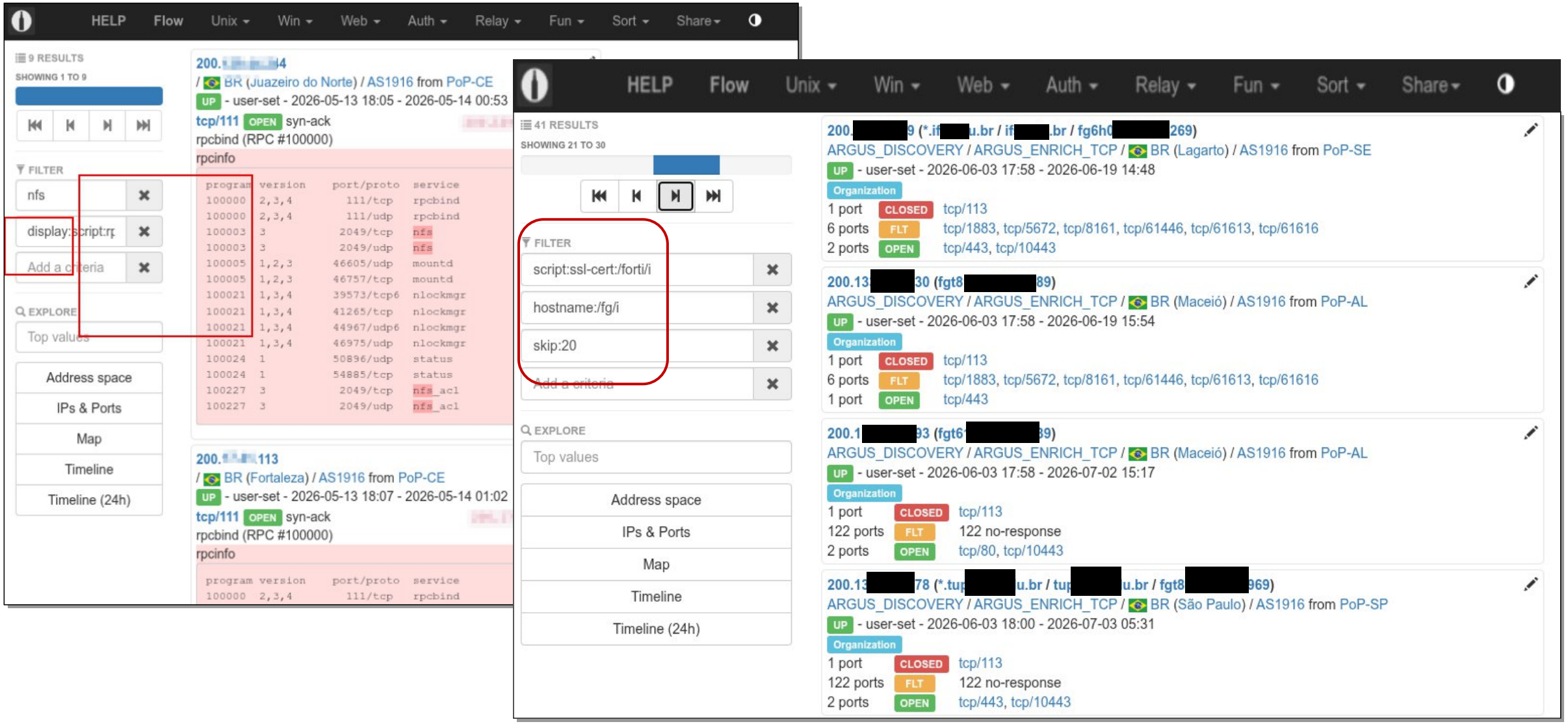
- *Comparativos*
- *Agregação*
- *Enriquecimento*
- *Histórico*



O IVRE não substitui as ferramentas citadas, ele "introduz" indexação, memória e contexto para os dados gerados.

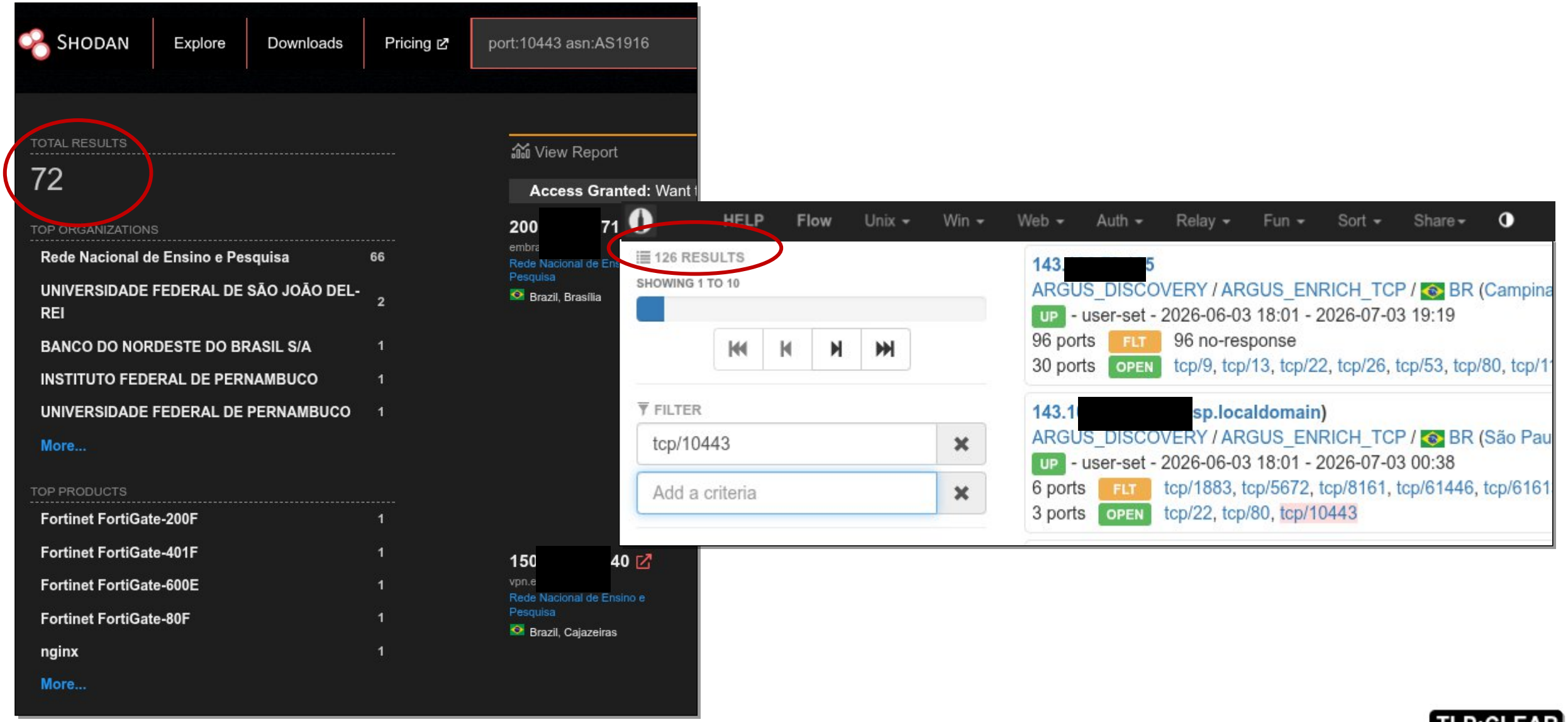
TLP:CLEAR

O que podemos fazer...



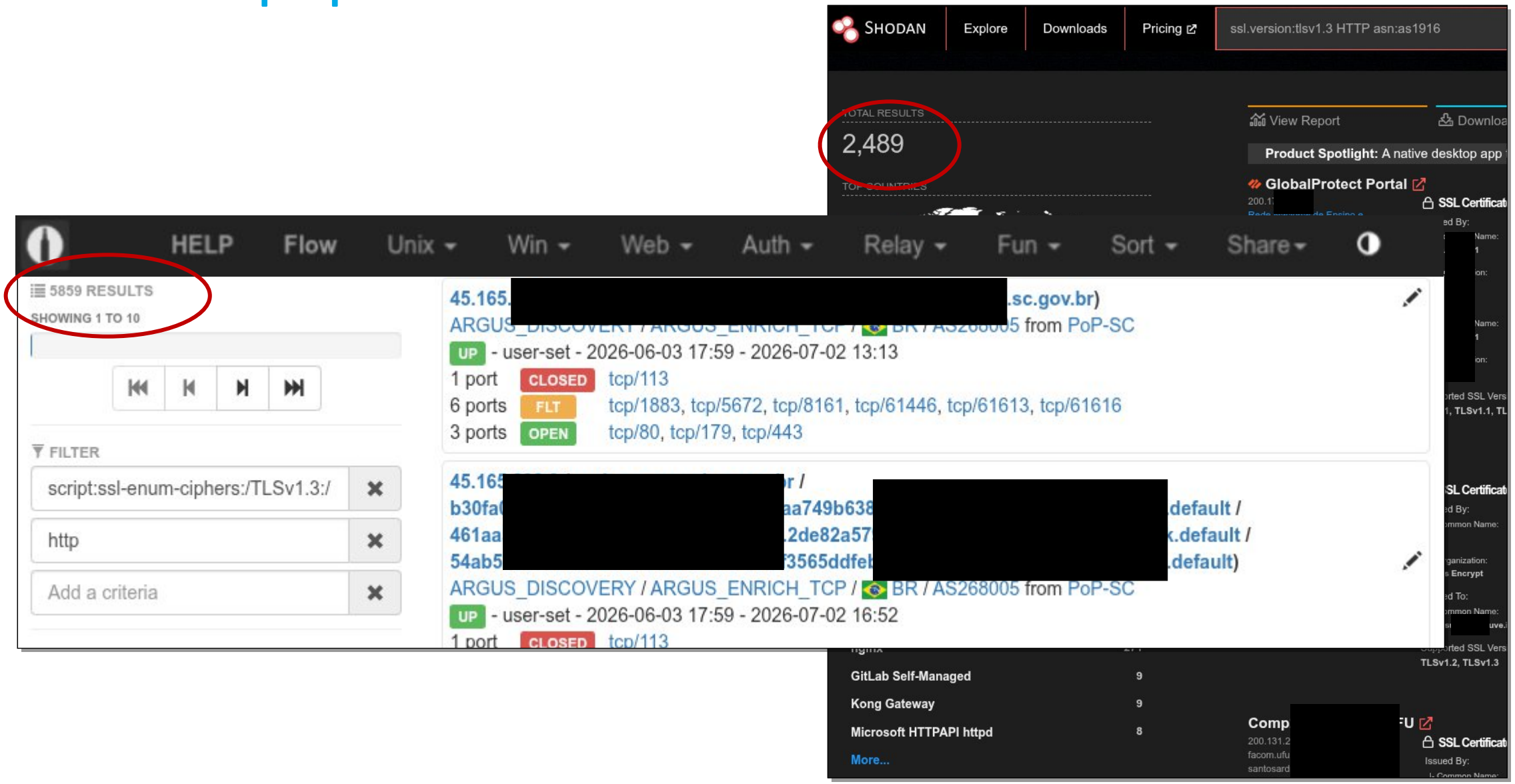
TLP:CLEAR

O que podemos fazer...



TLP:CLEAR

O que podemos fazer...



TLP:CLEAR

O que o IVRE NÃO é...

Scan pontual

- *Trata-se de uma base de conhecimento da superfície exposta ao longo do tempo.*

Uma ferramenta apenas "ofensiva" ou "defensiva"

- *É uma ferramenta muito útil para apoiar na validação e priorização.*

Não é um "inventário mágico"

- *Depende de escopo, recorrência, qualidade da coleta e interpretação.*

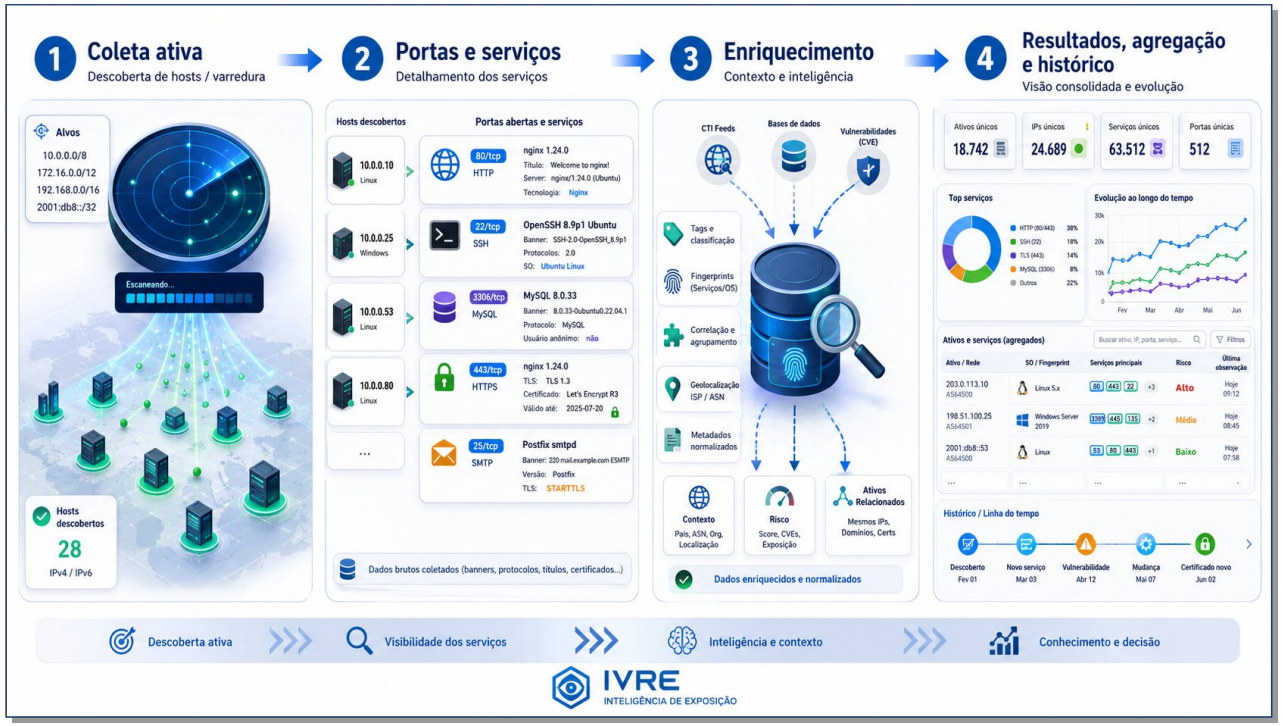
Coleta ativa: identificar “o que responde”

1 - Coleta ativa
- Descoberta de hosts
- Varredura

2 - Portas e serviços
- Detalhes dos serviços
- Protocolos
- Versões
- *Banners*

3 - Enriquecimento
- Contexto
- Inteligência
- Tags e classificação
- *Fingerprints*
- Correlação
- Geolocalização
- Metadados normalizados

4 - Resultados, agregação e histórico
- Visão consolidada
- Evolução
- Principais serviços
- Mudanças ao longo do tempo
- Risco
- Persistência
- Histórico



Descoberta ativa → Visibilidade de serviços → Inteligência e contexto → Conhecimento e tomada de decisão.

TLP:CLEAR

Coleta ativa: Cuidados!!!

Escopo explicito

- Redes autorizadas, janelas de execução, intensidade e exceções documentadas.

Impacto & Ritmo

- Varreduras precisam de controle de taxa (ex.: pacotes), *retry*, *timeout* e agenda.

Qualidade da informação

- *Banners* mentem! Versões podem estar mascaradas e falso positivo precisa de validação, por exemplo.

Governança

- Matriz RACI do processo.

Coleta passiva: Enxergar “o que acontece”

O que observa

- Eventos de rede
- Logs de serviços
  - DNS
  - SSH
  - HTTP
- Fluxos de rede

O que complementa

- Comunicação de saída
- Padrões de comunicação

Por que importa

- Pode não aparecer na varredura ativa.
- Pode estar visível no tráfego ou somente em janelas específicas.

Defesa realista

- Ativa: descobre o óbvio.
- Passiva: revela o que acontece.
- Histórica: mostra o que já aconteceu.

Menos pontos cegos. Mais contexto, melhores decisões.

TLP:CLEAR

Dados, perguntas e respostas...

Varredura

- *Hosts* descobertos
- Portas
- Serviços e *banners*
- Evidências

Passiva

- Evidências derivadas de *logs*
  - *DNS, SSH, HTTP, TLS...*

Fluxos

- Metadados de comunicação
- Análise temporal e volumetria

Visão

- Camada consolidada e correlacionada
- Cruzamento dados ativos, passivos e de fluxos

Perguntas que a visibilidade ajuda a responder

- O que está exposto?
- Com quem se comunica?
- O que mudou?
- Qual padrão é incomum?

Dados diferentes, finalidades diferentes. Compreensão completa. Respostas rápidas.

TLP:CLEAR

Projeto ARGUS RNP

Visibilidade recorrente da superfície exposta

- **Observar continuamente o backbone e identificar** *hosts*, portas, serviços e **mudanças relevantes**.

Histórico comparável de exposição

- Manter uma **linha do tempo** de portas, serviços, versões, *banners* e evidências **para análise de evolução e persistência**.

Insumos técnicos para decisão e priorização

- **Gerar dados acionáveis para *CTI*, *SOC* e times de segurança** de infraestrutura, **apoiando triagem, validação e resposta**.

Autonomia e soberania sobre os dados

- **Reduzir dependência de parceiros externos**, mantendo coleta, evidências e histórico sob controle da própria operação.

Alto valor técnico com baixo custo incremental

- Usar IVRE e **componentes *open-source*** para **transformar coleta recorrente** em **inteligência prática** sobre exposição.

Projeto ARGUS RNP

TLP:CLEAR

Onde o IVRE apoia SOC, Blue Team, CSIRT e CTI nas operações diárias.

1. Detectar exposição
2. Validar evidências
3. Contextualizar o risco
4. Acionar o responsável
5. Acompanhar o tratamento

Projeto ARGUS RNP

SOC

- Triagem rápida, enriquecimento de alertas e validação inicial.

Blue Team

- *Hunting* de superfície, baseline de serviços e validação de controles.

CSIRT

- Comunicação baseada em evidências, acompanhamento e lições aprendidas.

CTI

- Priorização, correlação externa e inteligência orientada ao ambiente.

Do achado à remediação: visibilidade, contexto e acompanhamento.

TLP:CLEAR

Projeto ARGUS RNP – Casos de uso

Sinais no IVRE

- *Host* ativo
- Porta / serviço aberto
- *Banner* de serviço
- *Hostname* inesperado
- Certificado estranho
- Produto fora do padrão

Ação esperada

- Validar responsável e finalidade
- Verificar a necessidade da exposição
- Revisar o controle de acesso
- Registrar no inventário
- Definir o tratamento e monitorar

Valor defensivo

- *Shadow IT*
- Laboratório esquecido
- *Appliance* exposto
- Serviço temporário que se tornou permanente

Pergunta principal:
O que está respondendo sem que ninguém esperasse?
Ativo desconhecido = incerteza operacional.

TLP:CLEAR

Projeto ARGUS RNP – Casos de uso

Da exposição à inteligência acionável

Observáveis técnicos do IVRE podem ser correlacionados para fins de investigação, formulação de hipóteses e tomada de decisões.

Observáveis

- IP / rede / ASN
- Portas / produtos
- Certificados TLS
- Chaves SSH
- DNS / hostnames
- Cabeçalhos HTTP

1 - Correlação

- KEV / EPSS
- MISP / AbuseIPDB
- Honeypots / Fluxo
- *Feeds* internos

2 - Hipóteses

- “Há exploração ativa?”
- “Este certificado aparece em outros locais?”

3 - Decisão

- Transformar dados técnicos em recomendações
- Recomendar: monitorar, notificar, bloquear, corrigir ou aceitar.

TLP:CLEAR

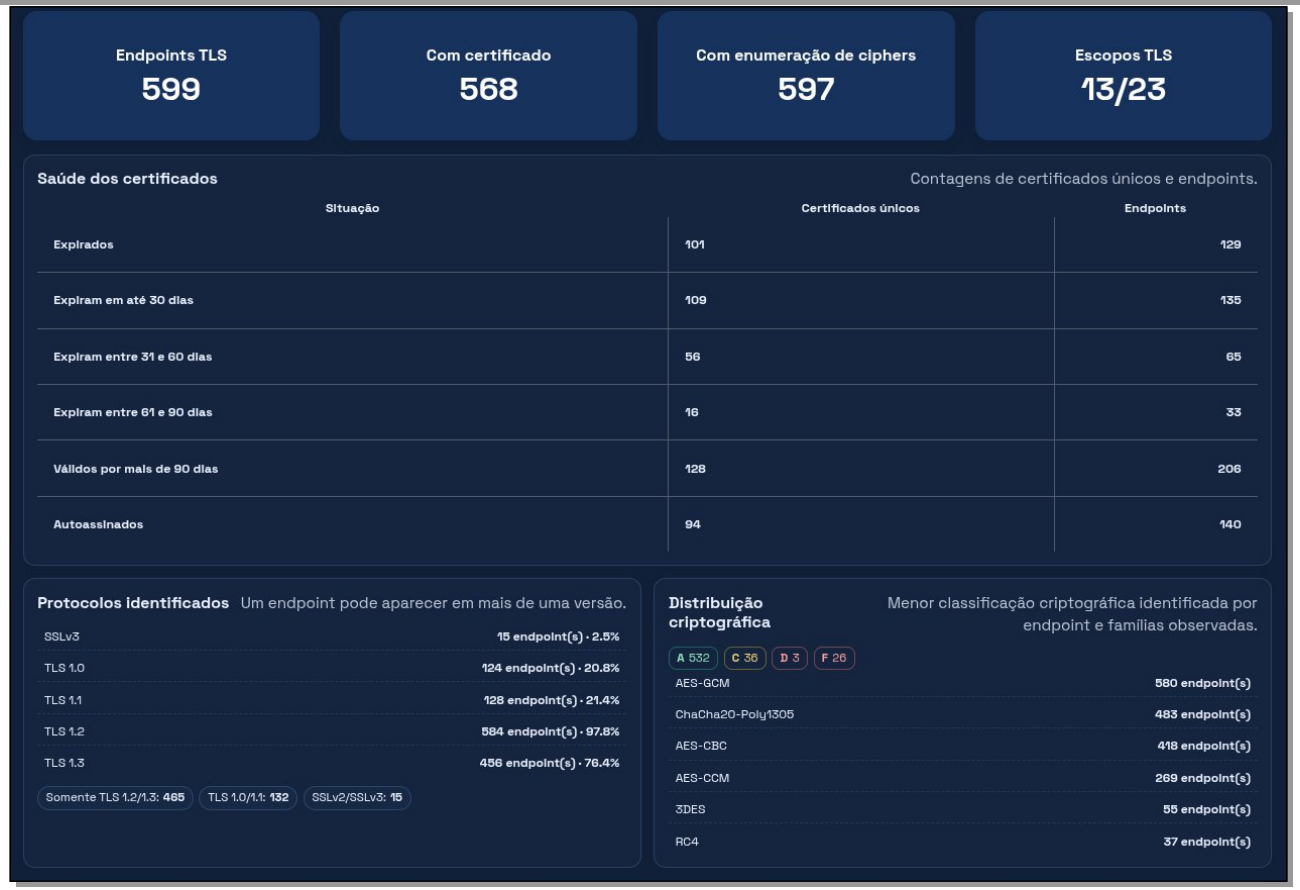
Projeto ARGUS RNP – Casos de uso

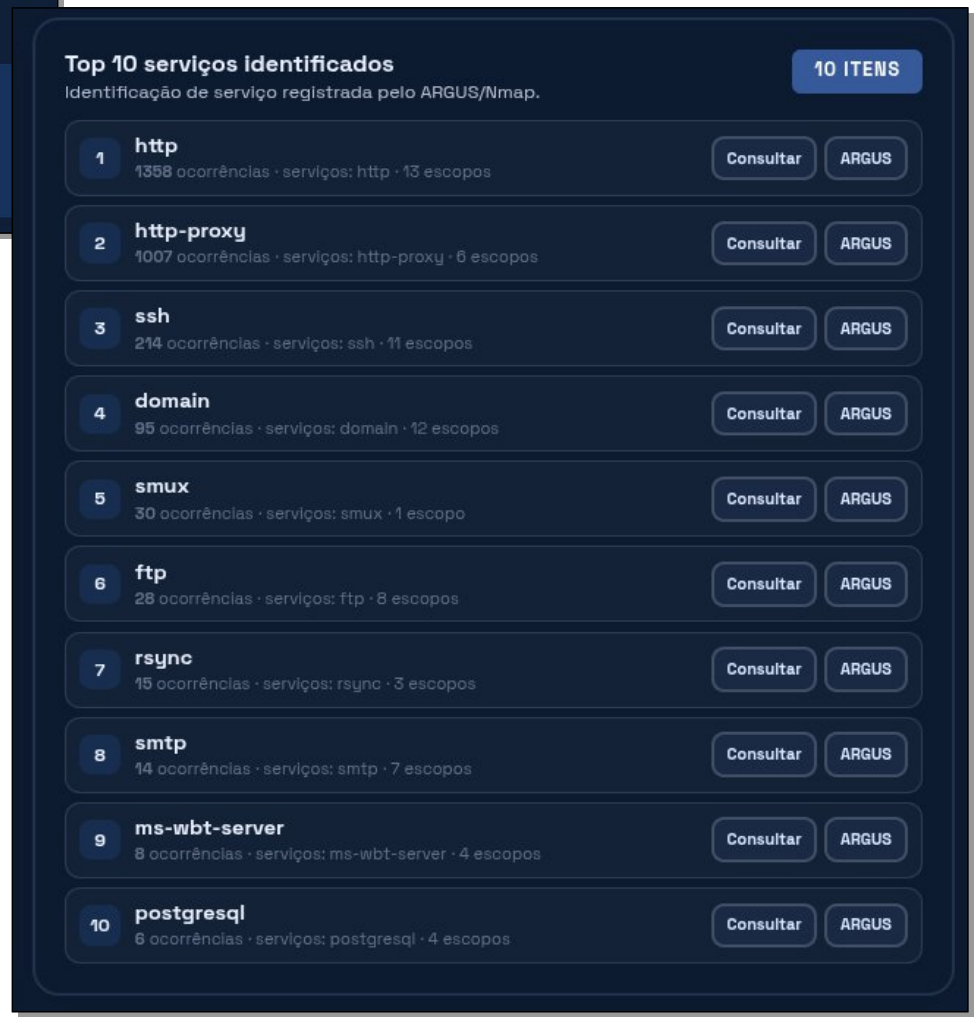
TLP:CLEAR

Projeto ARGUS RNP – Casos de uso

TLP:CLEAR

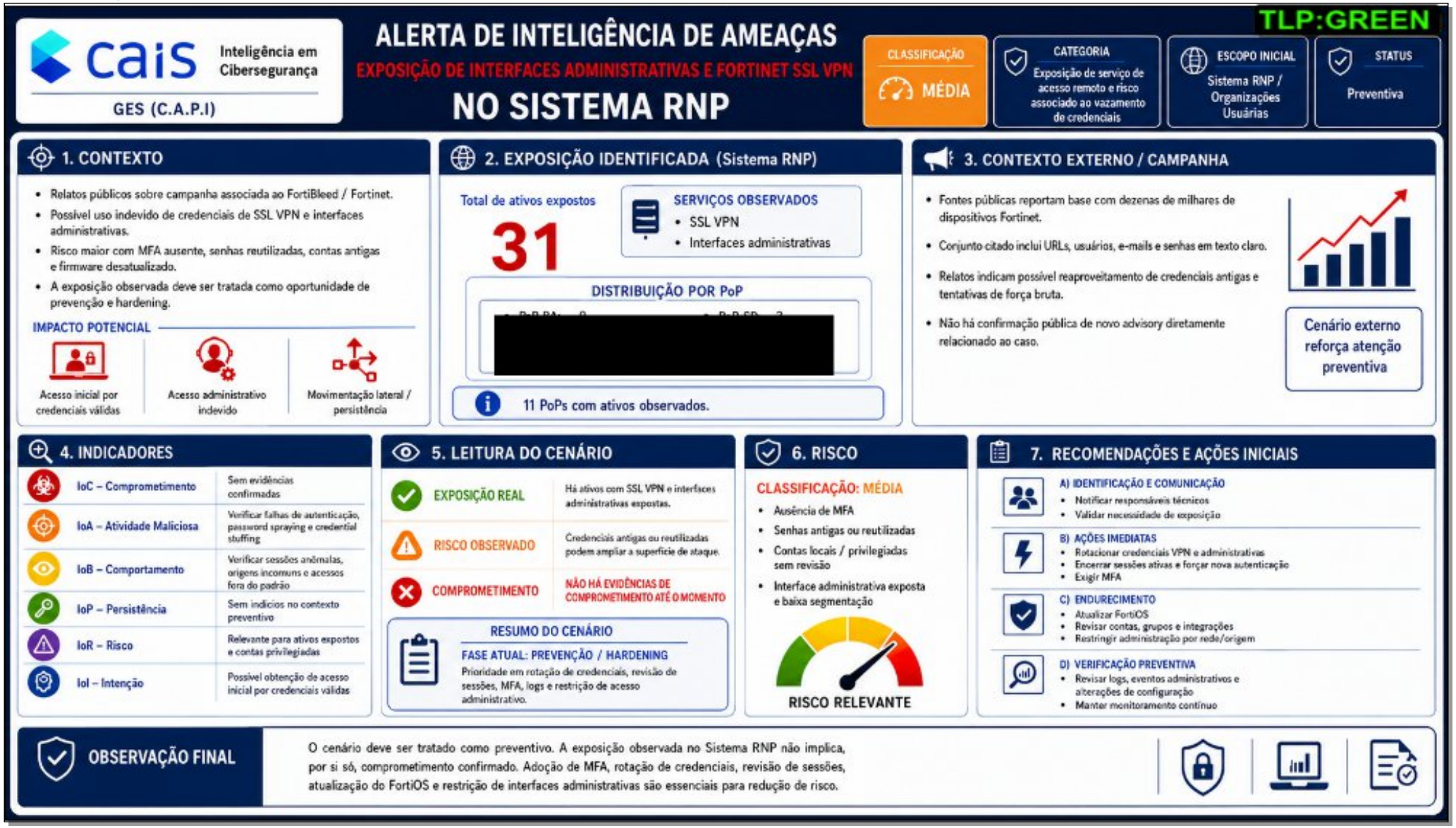
Projeto ARGUS RNP – Resultados...





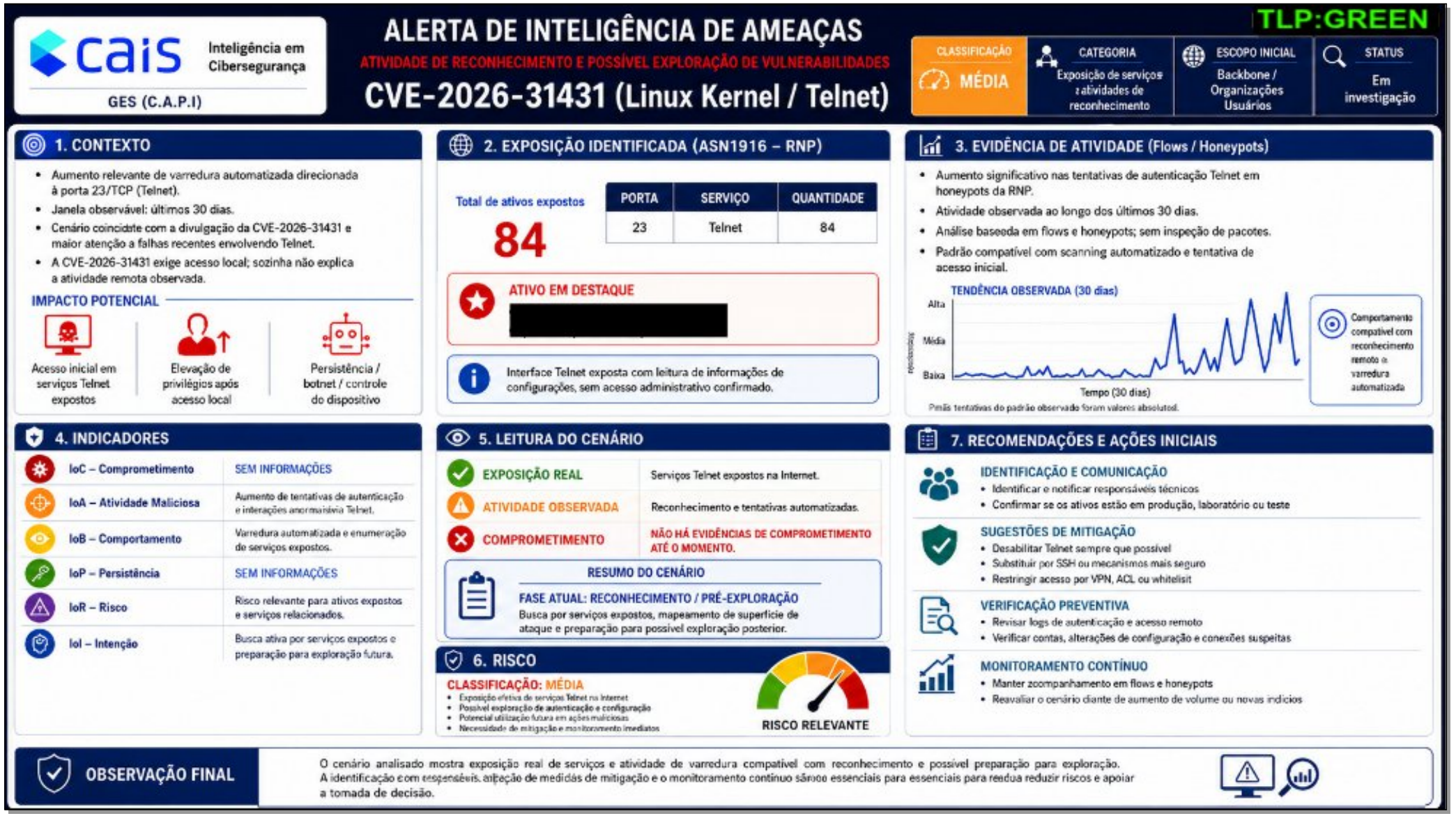
TLP:CLEAR

Projeto ARGUS RNP – Resultados...



TLP:CLEAR

Projeto ARGUS RNP – Resultados...



TLP:CLEAR

Projeto ARGUS RNP – Métricas (exemplos)

TLP:CLEAR

CONCLUSÃO

A superfície real de ataque não é estática nem totalmente conhecida. Deve ser observada de forma contínua, recorrente e comparável.

Visibilidade não é apenas inventário: é evidência técnica. Hosts, portas, serviços, versões, banners, certificados e mudanças mostram o que está efetivamente exposto.

Coletas ativa, passiva e histórica se complementam, reduzindo pontos cegos e separando achados isolados de exposições persistentes.

Dados brutos só viram prioridade quando são correlacionados com criticidade, recorrência, vulnerabilidades e explorabilidade.

Com evidências consistentes, Blue Team, SOC, CSIRT e CTI validam riscos, orientam notificações, acompanham o tratamento e medem a evolução.

OBRIGADO!!!

André R. **Landim**
andre.landim@rnp.br