



RiNIP

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/>

Sobre a RNP...

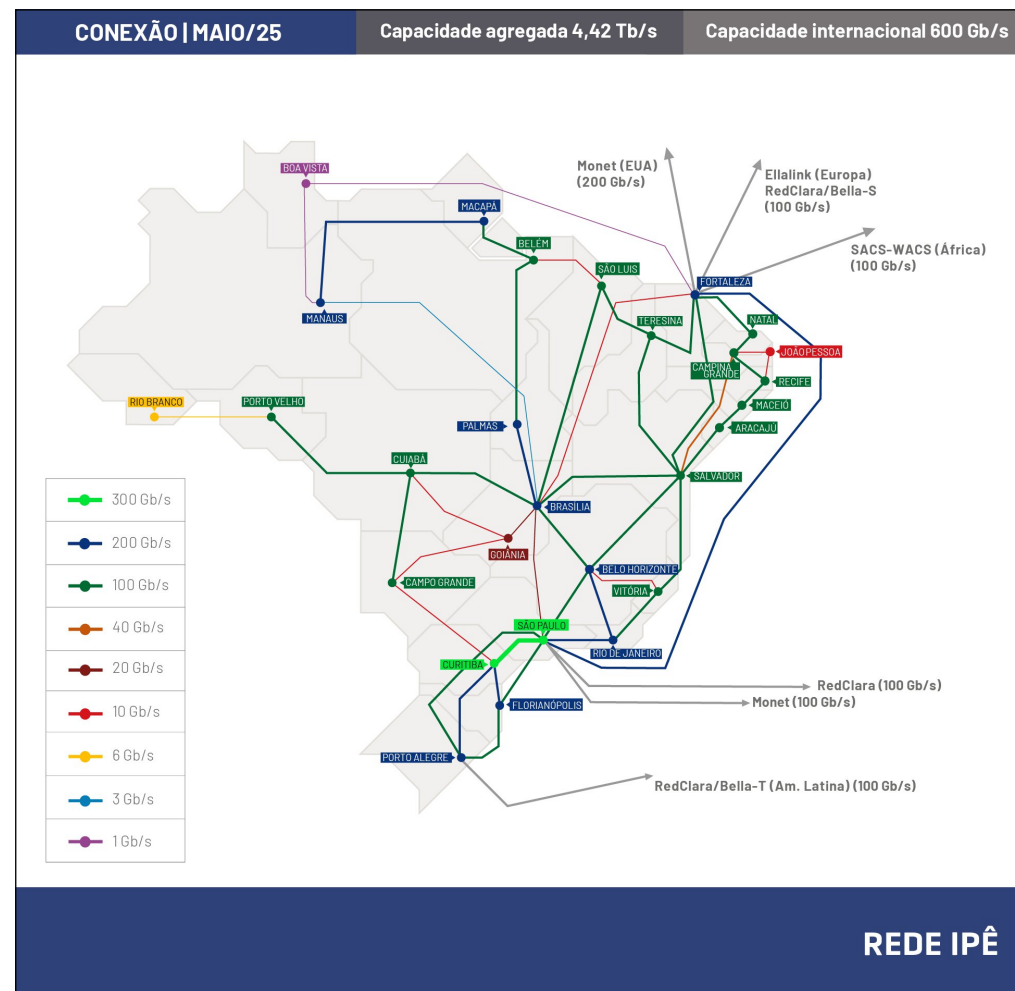


Conectamos universidades e instituições de ensino, pesquisa e inovação com internet e serviços seguros em uma comunidade, o Sistema RNP.

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.





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.



cais

**Inteligência em
Cibersegurança**



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



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



— 0 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/>

O que podemos fazer...



Coleta ativa / Enriquecimento

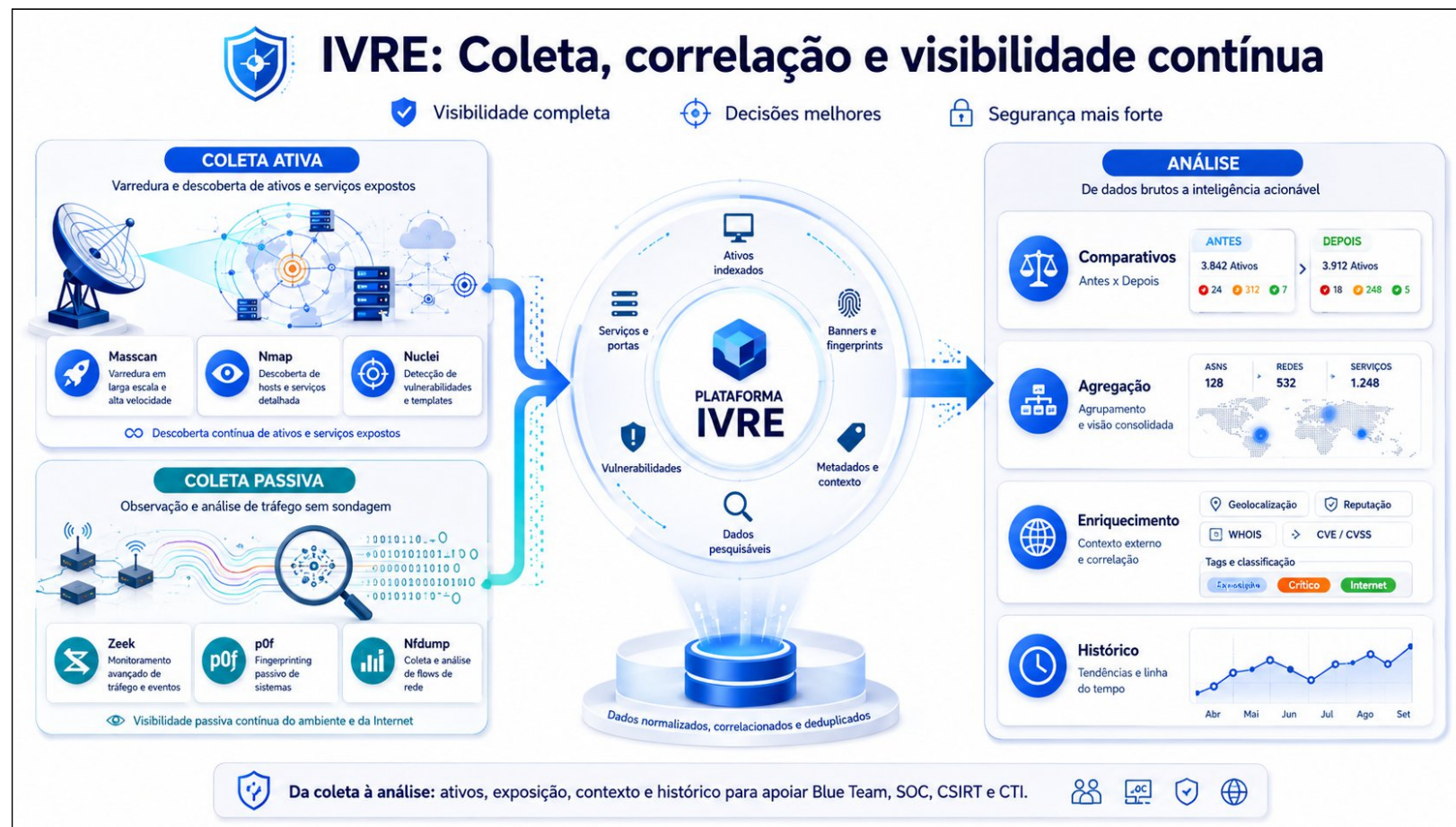
- Masscan
- NMAP
- Nuclei

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.

0 que podemos fazer...



9 RESULTS
SHOWING 1 TO 9

HELP Flow Unix Win Web Auth Relay Fun Sort Share

200.14
/ BR (Juazeiro do Norte) / AS1916 from PoP-CE
UP - user-set - 2026-05-13 18:05 - 2026-05-14 00:53
tcp/111 OPEN syn-ack
rpcbind (RPC #100000)
rpcinfo

FILTER

nfs

display:script:rpc

Add a criteria

Q EXPLORE

Top values

Address space

IPs & Ports

Map

Timeline

Timeline (24h)

program	version	port/proto	service
100000	2,3,4	111/tcp	rpcbind
100000	2,3,4	111/udp	rpcbind
100003	3	2049/tcp	nfs
100003	3	2049/udp	nfs
100005	1,2,3	46605/udp	mountd
100005	1,2,3	46757/tcp	mountd
100021	1,3,4	39573/tcp6	nlockmgr
100021	1,3,4	41265/tcp	nlockmgr
100021	1,3,4	44967/udp6	nlockmgr
100021	1,3,4	46975/udp	nlockmgr
100024	1	50896/udp	status
100024	1	54885/tcp	status
100227	3	2049/tcp	nfs_acl
100227	3	2049/udp	nfs_acl

200.113
/ BR (Fortaleza) / AS1916 from PoP-CE
UP - user-set - 2026-05-13 18:07 - 2026-05-14 01:02
tcp/111 OPEN syn-ack
rpcbind (RPC #100000)
rpcinfo

program	version	port/proto	service
100000	2,3,4	111/tcp	rpcbind

41 RESULTS
SHOWING 21 TO 30

HELP Flow Unix Win Web Auth Relay Fun Sort Share

200.9 (*.u.br / fg6h0269)
ARGUS_DISCOVERY / ARGUS_ENRICH_TCP / BR (Lagarto) / AS1916 from PoP-SE
UP - user-set - 2026-06-03 17:58 - 2026-06-19 14:48
Organization
1 port CLOSED tcp/113
6 ports FLT tcp/1883, tcp/5672, tcp/8161, tcp/61446, tcp/61613, tcp/61616
2 ports OPEN tcp/443, tcp/10443

200.130 (fgt889)
ARGUS_DISCOVERY / ARGUS_ENRICH_TCP / BR (Maceió) / AS1916 from PoP-AL
UP - user-set - 2026-06-03 17:58 - 2026-06-19 15:54
Organization
1 port CLOSED tcp/113
6 ports FLT tcp/1883, tcp/5672, tcp/8161, tcp/61446, tcp/61613, tcp/61616
1 port OPEN tcp/443

200.193 (fgt689)
ARGUS_DISCOVERY / ARGUS_ENRICH_TCP / BR (Maceió) / AS1916 from PoP-AL
UP - user-set - 2026-06-03 17:58 - 2026-07-02 15:17
Organization
1 port CLOSED tcp/113
122 ports FLT 122 no-response
2 ports OPEN tcp/80, tcp/10443

200.178 (*.tu.u.br / tu.u.br / fgt8969)
ARGUS_DISCOVERY / ARGUS_ENRICH_TCP / BR (São Paulo) / AS1916 from PoP-SP
UP - user-set - 2026-06-03 18:00 - 2026-07-03 05:31
Organization
1 port CLOSED tcp/113
122 ports FLT 122 no-response
2 ports OPEN tcp/443, tcp/10443

FILTER

script:ssl-cert:/forti/i

hostname:/fg/i

skip:20

Add a criteria

Q EXPLORE

Top values

Address space

IPs & Ports

Map

Timeline

Timeline (24h)

O que podemos fazer...



SHODAN

Explore

Downloads

Pricing

port:10443 asn:AS1916

TOTAL RESULTS

72

View Report

Access Granted: Want t

200

71

embra

Rede Nacional de Ens

Pesquisa

Brazil, Brasilia

TOP ORGANIZATIONS

Rede Nacional de Ensino e Pesquisa

66

UNIVERSIDADE FEDERAL DE SÃO JOÃO DEL-REI

2

BANCO DO NORDESTE DO BRASIL S/A

1

INSTITUTO FEDERAL DE PERNAMBUCO

1

UNIVERSIDADE FEDERAL DE PERNAMBUCO

1

More...

TOP PRODUCTS

Fortinet FortiGate-200F

1

Fortinet FortiGate-401F

1

Fortinet FortiGate-600E

1

Fortinet FortiGate-80F

1

nginx

1

More...

150

40

vpn.e

Rede Nacional de Ensino e Pesquisa

Brazil, Cajazeiras

HELP

Flow

Unix

Win

Web

Auth

Relay

Fun

Sort

Share

126 RESULTS

SHOWING 1 TO 10

⏮

⏪

⏩

⏭

FILTER

tcp/10443

×

Add a criteria

×

143.1

5

ARGUS_DISCOVERY / ARGUS_ENRICH_TCP / BR (Campina

UP - user-set - 2026-06-03 18:01 - 2026-07-03 19:19

96 ports FLT 96 no-response

30 ports OPEN tcp/9, tcp/13, tcp/22, tcp/26, tcp/53, tcp/80, tcp/11

143.1

sp.localdomain)

ARGUS_DISCOVERY / ARGUS_ENRICH_TCP / BR (São Pau

UP - user-set - 2026-06-03 18:01 - 2026-07-03 00:38

6 ports FLT tcp/1883, tcp/5672, tcp/8161, tcp/61446, tcp/6161

3 ports OPEN tcp/22, tcp/80, tcp/10443

— 0 que podemos fazer...



5859 RESULTS
SHOWING 1 TO 10

script:ssl-enum-ciphers:/TLSv1.3:/

http

Add a criteria

45.165. [REDACTED] .sc.gov.br)

ARGUS_DISCOVERY / ARGUS_ENRICH_TCP / [REDACTED] BR / AS268005 from PoP-SC

UP - user-set - 2026-06-03 17:59 - 2026-07-02 13:13

1 port CLOSED tcp/113

6 ports FLT tcp/1883, tcp/5672, tcp/8161, tcp/61446, tcp/61613, tcp/61616

3 ports OPEN tcp/80, tcp/179, tcp/443

45.165. [REDACTED] r /

b30fa [REDACTED] aa749b638 [REDACTED] default /

461aa [REDACTED] 2de82a57 [REDACTED] k.default /

54ab5 [REDACTED] 3565ddfel [REDACTED] .default)

ARGUS_DISCOVERY / ARGUS_ENRICH_TCP / [REDACTED] BR / AS268005 from PoP-SC

UP - user-set - 2026-06-03 17:59 - 2026-07-02 16:52

1 port CLOSED tcp/113

SHODAN

Explore

Downloads

Pricing

ssl.version:tlsv1.3 HTTP asn:as1916

2,489

View Report

Download

Product Spotlight: A native desktop app

GlobalProtect Portal

200.11

SSL Certificate

Issued By:

Name:

on:

orted SSL Vers

1, TLSv1.1, TL

SSL Certificat

ed By:

Common Name:

Organization:

Encrypt

ed To:

Common Name:

uve.

Supported SSL Vers

TLSv1.2, TLSv1.3

GitLab Self-Managed

9

Kong Gateway

9

Microsoft HTTPAPI httpd

8

Comp

200.131.2

facom.ufu

santosard

SSL Certificat

Issued By:

L. Common Name:

— 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

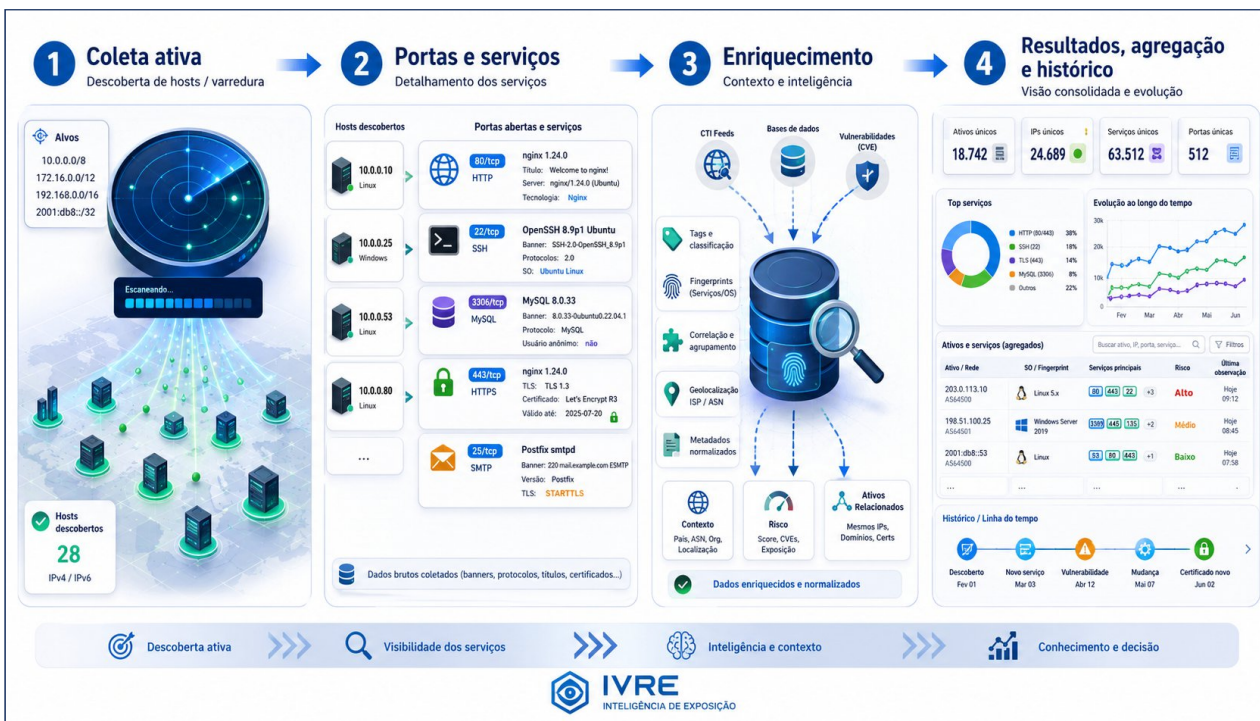
- Detalhes dos serviços
- Protocolos
- Versões
- *Banners*

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.**

— Coleta ativa: Cuidados!!!



Escopo explícito

- 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.**

— 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.



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



Projeto ARGUS na RNP: fluxo operacional com IVRE

Visibilidade contínua da superfície exposta para apoiar defesa, resposta e priorização



Do escopo à ação: o IVRE transforma coleta contínua em contexto, histórico e priorização para fortalecer a postura de segurança.



Cobertura ampla e responsável
foco na RNP e correlatos



Coleta controlada e ética
mínimo impacto, máximo valor



Inteligência com IVRE
dados correlacionados e pesquisáveis



Contexto histórico
tendências e mudança detectadas



Decisões melhores
risco reduzido, rede mais segura



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





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.**

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

Valor defensivo

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

Ação esperada

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



Pergunta principal:

**O que está respondendo sem que ninguém esperasse?
Ativo desconhecido = incerteza operacional.**



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.

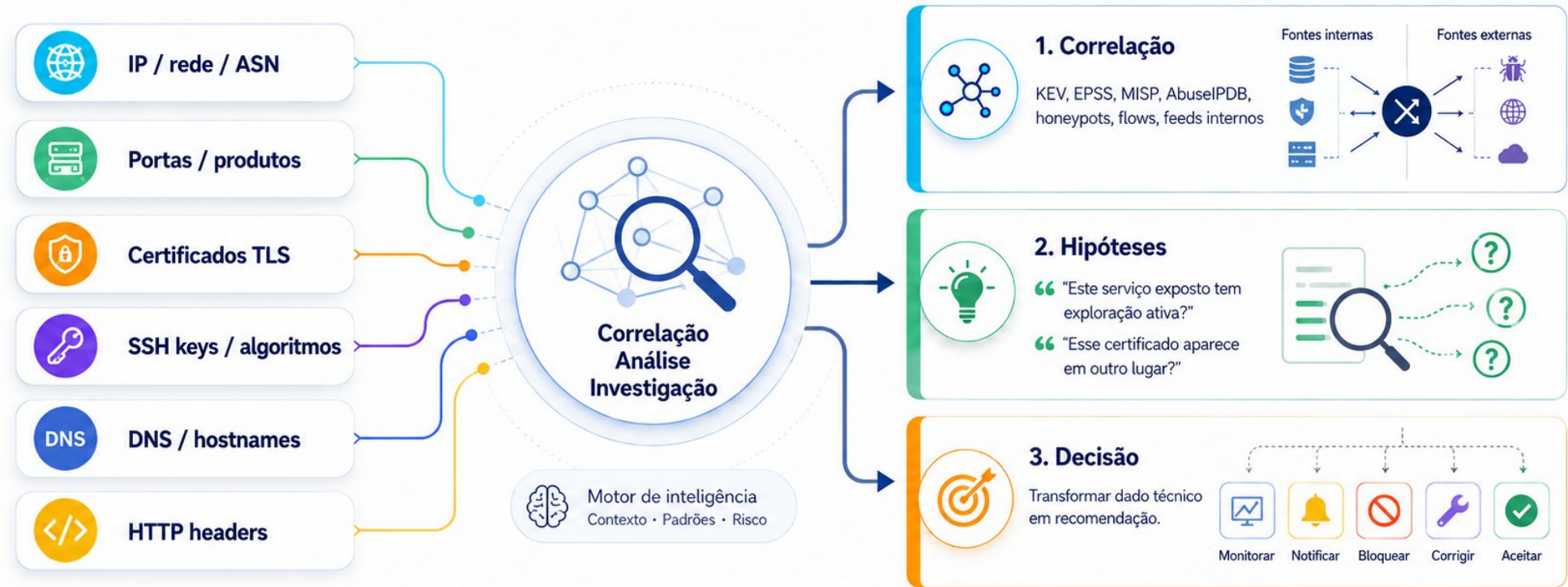


Projeto ARGUS RNP – Casos de uso



Da exposição para inteligência acionável

Observáveis técnicos do IVRE podem ser correlacionados para investigação, hipóteses e decisão.



O valor está em transformar observáveis dispersos em contexto, hipótese e ação.



Projeto ARGUS RNP – Casos de uso



CSIRT

Em incidente, IVRE responde perguntas rápidas

A base histórica ajuda a reconstruir exposição e escopo



Consulta operacional estruturada

Filtros

ASN / Escopo
AS1916

Serviço
Painel administrativo

Produto
Produto X

Versão
Y

Porta
8443

Estado
Exposto

Primeira observação
antes do alerta

Certificado / Fingerprint
similar

Rede / Faixa (opcional)
Ex.: 200.0.0.0/8 ou 200.0.0.0/16

Hosts correlatos

4 encontrados

Exportar

IP / Host	Porta	Produto	Versão	Primeira observação	Status atual
203.0.113.10	8443	Produto X	Y	2024-11-02 08:31	Exposto
203.0.113.27	8443	Produto X	Y	2024-11-02 09:12	Exposto
198.51.100.44	8443	Produto X	Y	2024-11-02 10:05	Exposto
198.51.100.88	8443	Produto X	Y	2024-11-02 12:46	Em correção
192.0.2.15	8443	Produto X	Y	2024-11-02 14:22	Corrigido

Linha do tempo histórica (visão agregada)

Primeira observação antes do alerta → Persistência da exposição até a mitigação → Após correção validação contínua



Do histórico ao filtro: contexto rápido para investigação, escopo e validação.





Projeto ARGUS RNP – Resultados...



Perfil da superfície Institucional

PoF

ARGUS / IVRE · VISÃO OBSERVADA · VÍNCULO POI

Perfil ARGUS parcial

Hosts com portas abertas

3403

Escopos com dados

13/23

Blocos consolidados

23

Backend

api

Endpoints TLS

599

Com certificado

568

Com enumeração de ciphers

597

Escopos TLS

13/23

Saúde dos certificados

Situação

Contagens de certificados únicos e endpoints.

	Certificados únicos	Endpoints
Expirados	101	129
Expiram em até 30 dias	109	135
Expiram entre 31 e 60 dias	56	65
Expiram entre 61 e 90 dias	16	33
Válidos por mais de 90 dias	128	206
Autoassinados	94	140

Protocolos identificados

Um endpoint pode aparecer em mais de uma versão.

SSLv3	15 endpoint(s) · 2.5%
TLS 1.0	124 endpoint(s) · 20.8%
TLS 1.1	128 endpoint(s) · 21.4%
TLS 1.2	584 endpoint(s) · 97.8%
TLS 1.3	456 endpoint(s) · 76.4%

Somente TLS 1.2/1.3: 485

TLS 1.0/1.1: 132

SSLv2/SSLv3: 15

Distribuição criptográfica

Menor classificação criptográfica identificada por endpoint e famílias observadas.

AES-GCM	580 endpoint(s)
ChaCha20-Poly1305	483 endpoint(s)
AES-CBC	418 endpoint(s)
AES-CCM	269 endpoint(s)
3DES	55 endpoint(s)
RC4	37 endpoint(s)

Top 10 serviços identificados

10 ITENS

Identificação de serviço registrada pelo ARGUS/Nmap.

1

http

1358 ocorrências · serviços: http · 13 escopos

Consultar

ARGUS

2

http-proxy

1007 ocorrências · serviços: http-proxy · 6 escopos

Consultar

ARGUS

3

ssh

214 ocorrências · serviços: ssh · 11 escopos

Consultar

ARGUS

4

domain

95 ocorrências · serviços: domain · 12 escopos

Consultar

ARGUS

5

smux

30 ocorrências · serviços: smux · 1 escopo

Consultar

ARGUS

6

ftp

28 ocorrências · serviços: ftp · 8 escopos

Consultar

ARGUS

7

rsync

15 ocorrências · serviços: rsync · 3 escopos

Consultar

ARGUS

8

smtp

14 ocorrências · serviços: smtp · 7 escopos

Consultar

ARGUS

9

ms-wbt-server

8 ocorrências · serviços: ms-wbt-server · 4 escopos

Consultar

ARGUS

10

postgresql

6 ocorrências · serviços: postgresql · 4 escopos

Consultar

ARGUS

Projeto ARGUS RNP – Resultados...



Projeto ARGUS RNP – Resultados...



TLP:CLEAR



Projeto ARGUS RNP – Métricas (exemplos)



Métricas que importam para superfície exposta

Medir para reduzir incerteza e apoiar ação — não apenas para enfeitar dashboards.



Cobertura de redes

Quanto do ambiente estamos de fato vendo.



↑ 8 p.p.
vs. mês anterior



Ativos/hosts novos

Novos ativos descobertos no período.



37
este mês
↓ 18% vs. mês anterior



Exposições críticas

Exposições com risco alto ou crítico.



24
no momento
▼ 12% vs. mês anterior



Persistência de exposição

Exposições que permanecem abertas por > 30 dias.



46%
acima de 30 dias
↑ 6 p.p. vs. mês anterior



Tempo de tratamento

Tempo médio para tratar exposições críticas.

7,6 dias

média dos últimos 30 dias
▼ 1,8 dias vs. mês anterior



Métrica útil

Transforma dados em direção.

Mostra o que priorizar, o que corrigir, como explicar e o que aprender.

Menos dúvidas, mais decisões.



Métrica ruim

Gera ruído e volume, não clareza.

Infla números, alimenta vaidade e não muda comportamento.

Muito dado, pouco impacto.



Objetivo prático

Parar de contar exposições e começar a responder:

Quais exposições, se reduzidas agora, diminuem mais risco?

Foco no impacto, não na quantidade.



Melhores métricas levam a melhores prioridades e menos incerteza.



Decisões mais assertivas



Redução real de risco



Progresso visível e sustentável

— 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



MINISTÉRIO DA
CULTURA

MINISTÉRIO DA
DEFESA

MINISTÉRIO DA
SAÚDE

MINISTÉRIO DAS
COMUNICAÇÕES

MINISTÉRIO DA
EDUCAÇÃO

MINISTÉRIO DA
CIÊNCIA, TECNOLOGIA
E INOVAÇÃO



TLP: CLEAR