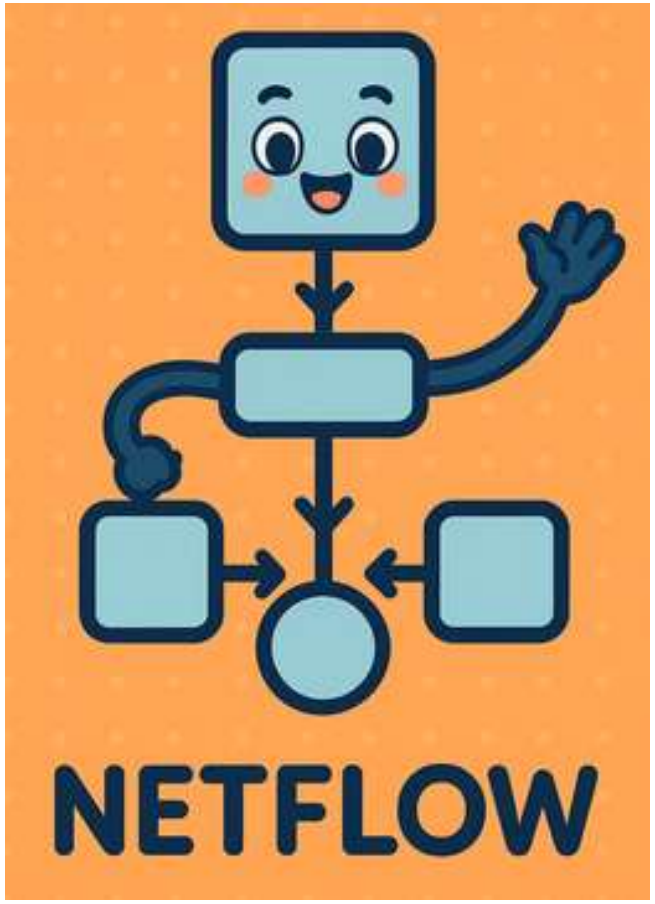
Uso de NetFlow no Contexto de Segurança e Tratamento de Incidentes em IF´s

Fórum CSIRT 2025 – Cert.br

TLP:CLEAR

Uso de NetFlow
no Contexto de Segurança e Tratamento de Incidentes em IF´s

Demonstrar a aplicação prática de NetFlow na segurança de Redes IF´s.



Imagens geradas com à SORA da OpenAI.

Edney Fernandes

Coordenador de Redes, CSIRT, Evangelizador Cybersegurança
Banco da Amazônia

www.linkedin.com/in/edneyfer

TLP:CLEAR

Contexto atual nas IF´s

Crescimento das Ameaças Cibernéticas

SOFISTICAÇÃO BRUTAL

ORGANIZAÇÕES CRIMINOSAS

Ransomware-as-a-Service (RaaS)

A ameaça interna (insider threat)

Ataques de supply chain → Softwares bancários e de integração financeira.

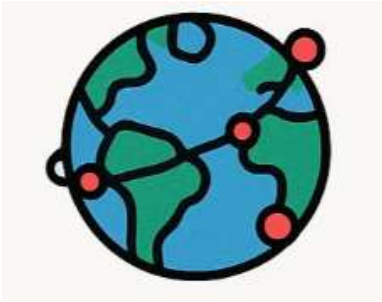
TLP:CLEAR

Contexto atual nas IF´s

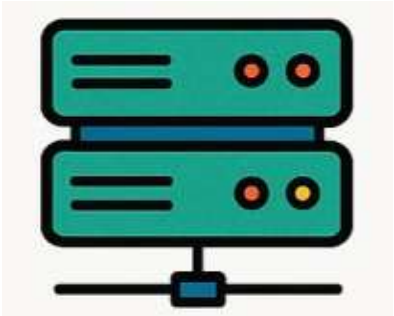
Complexidade dos Ambientes Bancários
Redes bancárias:

Agências físicas (centenas pontos)

ATMs



Interconexão de compensação (ex: SWIFT)



Data Centers

Ambientes de nuvem híbrida

TLP:CLEAR

Contexto atual nas IF´s

Pressão Regulamentar e Conformidade

Banco Central (BACEN Resolução 4.893)

- Detecção de ataques
- Procedimentos formais
- Retenção de registros

LGPD (Lei Geral de Proteção de Dados):

- Exige rastreabilidade completa em incidentes de vazamento de dados.

Normas internacionais com forte peso sobre auditoria de logs e análise de tráfego.

TLP:CLEAR

Contexto atual nas IF´s

O Desafio da Visibilidade

Começa a dor real para o SOC e para o CSIRT:

Grande parte do tráfego interno não é visível.

Muitos movimentos laterais não geram alertas tradicionais.

Passam despercebidos se a instituição não tiver visibilidade de rede.

O que é NetFlow e como funciona

O que o NetFlow coleta?

Tecnologia de **exportação de metadados** de tráfego IP

Resume sessões de comunicação em registros compactos chamados *flows* (fluxos).

O que é NetFlow e como funciona

🧠 O que define um “fluxo” no NetFlow?

IP de Origem
Quem iniciou a comunicação

IP de Destino
Quem recebeu a comunicação

Porta de Origem
Porta aleatória usada pelo cliente para sair

Porta de Destino
Porta do serviço acessado (ex: 443, 22, 25)

Protocolo
Tipo de protocolo utilizado (ex: TCP, UDP, ICMP)

TLP:CLEAR

O que é NetFlow e como funciona

Tipos e Versões

v5 — NetFlow v5 — Campos fixos, básico
Campos básicos (IP, porta, protocolo)

IPv6 v9 — NetFlow v9 — Campos flexíveis, templates

IPv6 — IPFIX — Padrão IETF aberto (RFC 7011–7015)

IPv6 — sFlow (Sampled Flow) — (RFC 3176), mantido pela sFlow.org

IPv6 — jFlow (Juniper Flow Monitoring), Equipamentos Juniper
Compatível com NetFlow v5/9, adaptado aos equipamentos Juniper

Criado Cisco 1990
NetFlow v1, v5, v7 e v9

Ex: Netflow

```
{
  "srcaddr": "192.168.0.10",
  "dstaddr": "172.217.28.238",
  "srcport": 54321,
  "dstport": 443,
  "prot": 6,
  "tcp_flags": 0x1B,
  "packets": 12,
  "bytes": 6543,
  "start_time": "2025-07-27 12:01:45.321",
  "end_time": "2025-07-27 12:01:48.531",
  "src_mask": 24,
  "dst_mask": 24,
  "src_as": 0,
  "dst_as": 15169
}
```

FIN(0x01), SYN(0x02), PSH(0x08), ACK(0x10)

TLP:CLEAR

O que é NetFlow e como funciona

⚠️ **Importante Diferenciação Técnica**

❌ NetFlow ≠ IDS

❌ NetFlow ≠ Full Packet Capture (PCAP)

❌ NetFlow ≠ Firewall logs

🧮 **Resumo Estatístico de Tráfego**

Não vê o "qué" foi transmitido

Vê "quem falou com quem, quando e por quanto tempo

O que é NetFlow e como funciona

🎯 O diferencial estratégico

Tráfego criptografado
(TLS 1.3, VPN IPsec,
HTTPS, etc.)

NetFlow continua observando
esses metadados.

Quantidade
de Sessões

Volume de
Dados

Frequência e
Periodicidade

Destinos
Não Usuais

TLP:CLEAR

Por que NetFlow é estratégico em IF´s

⚠️ Ataques não param na porta de entrada

Tudo ocorre debaixo do radar!

Sistemas tradicionais como firewalls, EDR, IDS muitas vezes não detectam essas etapas.

TLP:CLEAR

Por que NetFlow é estratégico em IF´s

Onde o NetFlow entrega visibilidade nesse contexto?

NetFlow
Câmera de Segurança da Rede

Captura de
Relacionamentos

Comunicações
Incomuns

Exfiltração
de Dados

Linha do Tempo
de Eventos

Beaconing de
Malware

TLP:CLEAR

Por que NetFlow é estratégico em IF´s

Visibilidade de tráfego mesmo criptografado

Tráfego Criptografado = 90% da rede (*(TLS 1.2, TLS 1.3, IPsec, VPN, HTTPS).*

DPI (*Deep Packet Inspection*) ≠ Viável em ambiente interno

NETFLOW FUNCIONA SEM VER PAYLOAD

Metadados Observáveis pelo NetFlow

- IP de origem e destino
- Portas utilizadas
- Volume de dados
- Sessões e tempo de duração

Por que NetFlow é estratégico em IF´s

Contexto Regulatórios:

Exigem rastreabilidade

NetFlow permite auditoria mesmo após o incidente

Suporte forense com profundidade

Fortalecimento do SOC e CSIRT:

Prova técnica

Hunting ativo guiado por tráfego

Zero Trust e Microsegmentação com validação contínua

TLP:CLEAR

Por que NetFlow é estratégico em IF´s

Comportamento ≠ Conteúdo

Beaconing

Novos relacionamentos

Comunicação inter-agências

Sessões anômalas

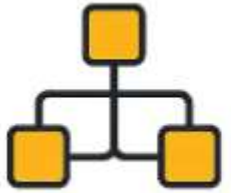
NetFlow vé tudo isso.

Logs de firewall/IDS não.

TLP:CLEAR

Como o NetFlow Atua no Ciclo de Incidentes

DETECÇÃO
Visibilidade Inicial com NetFlow



CONTENÇÃO
Resposta Baseada em Fluxos

ERRADICAÇÃO
Monitoramento Pós-Mitigação

LIÇÕES APRENDIDAS
Forense com NetFlow

Como o NetFlow Atua no Ciclo de Incidentes

🔍 DETECÇÃO — Visibilidade Inicial com NetFlow

👁️ NetFlow detecta o que firewall e IDS ignoram:

🕵️ Ajuda a identificar:

Como o NetFlow Atua no Ciclo de Incidentes

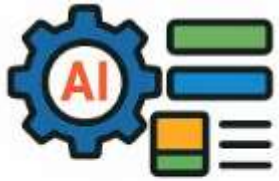
CONTENÇÃO — Resposta Baseada em Fluxos

Quem mais falou com o IP X ?

Quais sub-redes foram afetadas?

Mapeamento do blast radius

Regras de firewall cirúrgicas



SOAR automatiza bloqueios com dados NetFlow

Exemplo: IP comprometído → lístar conexões → bloquear com precisão

Como o NetFlow Atua no Ciclo de Incidentes

ERRADICAÇÃO — Monitoramento Pós-Mitigação

Tráfego anômalo cessou?

Malware tentando se reconectar?

Canais alternativos sendo usados?

Validação da limpeza REAL

Exemplo: Após remoção de exfiltração DNS, NetFlow detecta máquinas replicando o padrão

Como o NetFlow Atua no Ciclo de Incidentes

LIÇÕES APRENDIDAS — Forense com NetFlow

Linha do tempo do incidente

Vetor de entrada identificado

Apoia auditorias (BACEN, LGPD)

Relatórios para diretoria

Melhoria nos controles

TLP:CLEAR

Topologia em IF´s

Onde Ativar NetFlow

Agencias / ATM
(Switch L3 NetFlow)

WAN/MPLS/VPN
(Router NetFlow)

Firewalls / Borda
(NGFW NetFlow)

DMZ / Balanceadores
(IPFIX)

Core DC
(Switch Core NetFlow)

Cloud
(VPC Flow Logs)

TLP:CLEAR

Arquitetura de Coleta

🧱 Arquitetura NetFlow — 3 Blocos Funcionais

Dispositivos que geram e enviam os flows (switch, router, loadbalances, firewall, cloud)

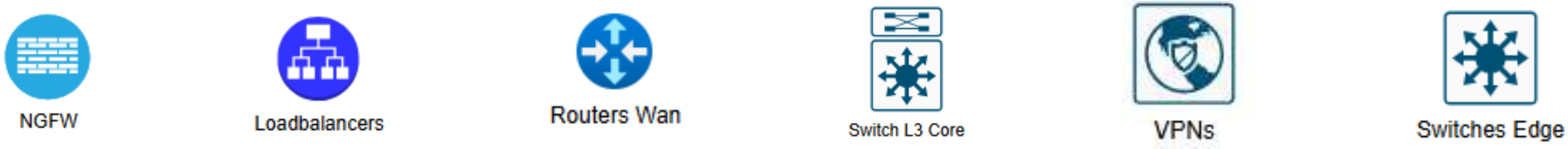
Servidores que recebem, organizam e armazenam os dados de fluxo
Ex: Stealthwatch (Cisco) , Trafip (Telcomanager), Elastic Stack (ELK)

Ferramentas (NDR e SIEM) que analisam os flows e geram insights para o SOC.
Ex. Scrutinizer (Plixer), Flowmon (Progress), Darktrace, Vectra AI

TLP:CLEAR

Arquitetura Técnica de Coleta

Exportadores NetFlow/IPFIX/sFlow/jFlow



Suporte nativo:

FORTINET
CISCO
CHECK POINT
paloalto NETWORKS
juniper NETWORKS

TLP:CLEAR

Arquitetura Técnica de Coleta

🎯 **Coletor (Collector)**
O coletor centraliza os fluxos exportados e armazena para análise.

Funções principais:
🛰️ Receber grandes volumes de fluxos (em UDP ou TCP).
📦 Indexar e armazenar dados de forma eficiente.
🔍 Permitir consultas retroativas e geração de alertas.

🛠️ **Exemplos de ferramentas de mercado:**

Comercial

cisco Stealthwatch

PLIXER

Flowmon
Driving Network Visibility

Open-Source

ntopng / nProbe

elastic + logstash + kibana

TLP:CLEAR

Arquitetura Técnica de Coleta

🔍 **Funções:**

🔗 Correlação com IOCs/logs | 📊 Baselines comportamentais

🚨 Alertas dinâmicos | 🎯 Hunting proativo

🧠 Analyzer (Analisador)

SIEM

QRadar splunk> ArcSight

Agregam, correlacionam e investigam múltiplas fontes de log.

NDR

DARKTRACE CISCO Stealthwatch VECTRA™

Detectam ameaças com foco em comportamento de rede.

TLP:CLEAR

Caso Simulado 1: Exfiltração via DNS Túnel

1️⃣ Comprometimento Inicial

O atacante obtém acesso inicial à rede ou estação.

Vetores comuns:

- 🎣 **Phishing**
- 🐛 **Zero-day**
- 🔐 **VPN com credencial válida**

2️⃣ Persistência e Estudo do Ambiente

O malware se instala de forma durável e começa a mapear o ambiente interno.

Ações típicas:

- 📂 Diretórios mapeados
- 📄 Arquivos de clientes

3️⃣ Exfiltração Furtiva via DNS

Em vez de FTP ou HTTP, os dados são exfiltrados via requisições DNS disfarçadas.

Exemplo:

🧬 🅱️ 🔡 Base64DoArquivo.exfil.credito-rural[.]com

4️⃣ Estação → DNS interno → Internet → DNS do atacante

TLP:CLEAR

Caso Simulado 1: Exfiltração via DNS Túnel

Como NetFlow detecta exfiltração via DNS

📦 **UDP 53 em massa**
📡 Workstation infectada
📈 Centenas/milhares de queries por minuto

Start Time	End Time	Src IP	Dst IP	Proto	SrcPort	DstPort	Packets	Bytes	Flags
2025-07-23 14:32	2025-07-23 14:35	10.0.5.42	185.100.87.1	UDP	53421	53	670	199800	-
2025-07-23 14:32	2025-07-23 14:35	10.0.5.42	185.100.87.1	UDP	53422	53	645	193500	-
2025-07-23 14:32	2025-07-23 14:35	10.0.5.42	185.100.87.1	UDP	53423	53	660	197000	-
2025-07-23 14:32	2025-07-23 14:35	10.0.5.42	185.100.87.1	UDP	53424	53	688	206400	-
2025-07-23 14:32	2025-07-23 14:35	10.0.5.42	185.100.87.1	UDP	53425	53	702	210600	-
2025-07-23 14:32	2025-07-23 14:35	10.0.5.42	185.100.87.1	UDP	53426	53	695	208500	-
2025-07-23 14:32	2025-07-23 14:35	10.0.5.42	185.100.87.1	UDP	53427	53	675	200100	-
2025-07-23 14:32	2025-07-23 14:35	10.0.5.42	185.100.87.1	UDP	53428	53	690	205200	-

🔐 **Mesmo com DNS criptografado (DoH/DoT), volume ainda é anômalo**

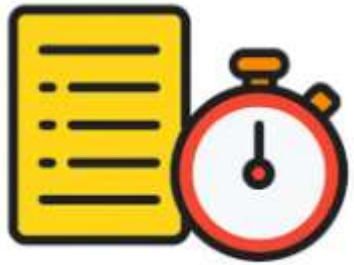
Caso Simulado 1: Exfiltração via DNS Túnel

SOC investigando com NetFlow

1

Alerta DNS Anômalo

2



SOC analisa

Quais IPs geraram os fluxos.
Quais servidores de DNS foram acionados.
Quando o comportamento iniciou.

3

Correlação

Logs de endpoint.
Identificação do usuário daquela estação.

4

Confirma exfiltração por DNS

5

Contenção rápida e precisa

Bloqueia comunicação
Bloqueia estação do usuário

TLP:CLEAR

Caso Simulado 2: Acesso não Autorizado a Sistemas Core

Caminho do Ataque

Terminal de agência (ex: gerente)

Escalada de privilégios / caminhos indevidos

Estação acessa sistemas core banking (Crédito, Cadastro)

🚨 **Consequência:**

- 🚫 Violação de função
- 🕵️ Risco de fraude ou vazamento
- ⚖️ Não conformidade

TLP:CLEAR

Caso Simulado 2: Acesso não Autorizado a Sistemas Core

👁️ NetFlow detecta comportamento anômalo

Start Time	End Time	Src IP	Dst IP	Proto	SrcPort	DstPort	Packets	Bytes	Flags
2025-07-23 01:12	2025-07-23 01:45	192.168.10.45	10.1.1.100	TCP	50932	1433	860	97000	AP
2025-07-23 01:13	2025-07-23 01:46	192.168.10.45	10.1.1.120	TCP	50933	1521	905	108000	AP
2025-07-23 01:14	2025-07-23 01:47	192.168.10.45	10.1.2.135	TCP	50934	3306	780	88000	AP
2025-07-23 01:14	2025-07-23 01:50	192.168.10.45	10.1.1.1	TCP	50935	22	620	53000	S
2025-07-23 01:15	2025-07-23 01:53	192.168.10.45	10.1.1.104	TCP	50936	3389	870	210000	PA
2025-07-23 01:16	2025-07-23 01:54	192.168.10.45	10.1.1.105	TCP	50937	443	900	124000	AP
2025-07-23 01:17	2025-07-23 01:48	192.168.10.45	10.1.0.10	TCP	50938	8080	740	66000	AP
2025-07-23 01:18	2025-07-23 01:49	192.168.10.45	10.1.5.10	TCP	50939	5900	520	44000	S
2025-07-23 01:19	2025-07-23 01:51	192.168.10.45	10.1.1.75	TCP	50940	21	610	72000	PA
2025-07-23 01:20	2025-07-23 01:55	192.168.10.45	10.1.1.200	TCP	50941	8443	830	91000	AP

🚩 **Desvio de perfil:**
👩‍💻 A estação nunca acessou esse servidor
👄 O setor não usa esse sistema

TLP:CLEAR

Caso Simulado 2: Acesso não Autorizado a Sistemas Core

NetFlow enxerga:

Comunicação inesperada

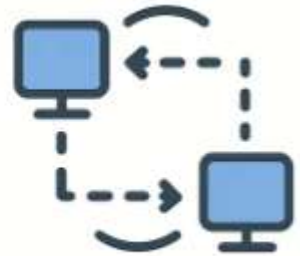
Relações fora do padrão

Por que Firewall / IDS falham?

Tráfego é permitido

Sem assinatura ativada

Fluxo interno, não visível no perímetro



TLP:CLEAR

Caso Simulado 3: Movimentação Lateral

🧨 Como o Ataque Ocorre

1️⃣ 🎣 Compromete endpoint com acesso limitado
2️⃣ 🧭 Reconhecimento interno (varredura, enumeração)
3️⃣ 🔓 Coleta novas credenciais (LSASS, senhas, shares)
4️⃣ ↔️ Movimento lateral (RDP, SMB, WMI, SQL)
5️⃣ 🎯 Alvo: AD, file servers, core bancário;

👁️ **NetFlow detecta movimento lateral via padrões de tráfego:**

🌐 IP Origem: Host comprometido
🖧 IP Destino: Diversos hosts internos
📦 Portas: 445, 3389, 5985, 135, 1433...
📶 Protocolo: TCP
📈 Frequência: Conexões rápidas e em massa
⚡ Duração: Fluxos curtos para teste de autenticação

Caso Simulado 3: Movimentação Lateral

⚠️ Padrões Anômalos Comuns

🔁 Múltiplos destinos em curto tempo
🔐 Protocolos não esperados para o perfil
🤝❌ Hosts que não costumam interagir
🌙 Atividades fora do expediente
🤖 Padrões “não humanos” (sequência exata de tempo)

📊 Exemplo:
23:42:10 → IP .101 porta 445
23:42:11 → IP .102 porta 445
23:42:12 → IP .103 porta 3389

StartTime: 23:42:10.100
📍 SrcIP: 10.20.30.50 → (🖥️ estação comprometida)
🎯 DstIP: 10.20.30.101 → Port 445 → (📁 SMB)
📦 2 packets / 300 bytes

StartTime: 23:42:11.050
🎯 DstIP: 10.20.30.102 → Port 445

StartTime: 23:42:12.100
🎯 DstIP: 10.20.30.103 → Port 3389 (🖥️ RDP)

Caso Simulado 3: Movimentação Lateral

👁️ **NetFlow enxerga:**

🔄 Relacionamentos incomuns entre hosts

📈 Padrões repetitivos, portas críticas

❓ **Por que Firewalls/IDS falham?**

1️⃣ 🔁 Tráfego interno (intra-sub-rede)

2️⃣ 🔓 Políticas permitem RDP/SMB internamente

3️⃣ 🔬 IDS vê payload — e o atacante só tenta logon

👁️ **Detecção de Anomalias com NetFlow**

🔄 Fluxos laterais não esperados

🔍 Enumeração rápida (scans internos)

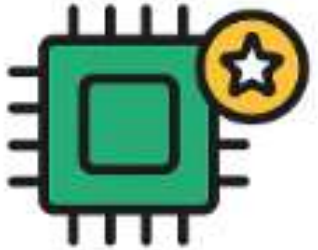
🕵️ Acesso fora do perfil de host/usuário

🌙 Atividade fora de horário (turno incomum)

Boas Práticas de Implementação

Planejamento de Coleta

\+ pontos de coleta = + visibilidade



Enriquecimento de NetFlow

NetFlow v9/IPFIX ativo

Recomendação:

NetFlow v9 IPFIX

sempre que possível

Boas Práticas de Implementação

Integrar o NetFlow com ecossistema SOC

SIEM (correlação de alertas/logs)

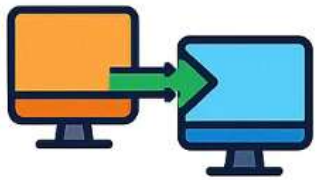
NDR (detecção comportamental)

SOAR (resposta automatizada)

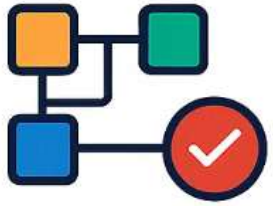
Atenção com segmentação e NAT

Atenção com segmentação e NAT

Registrar traduções no SIEM



Corrigir IP lógico nos fluxos



NetFlow pós-NAT para rastreabilidade

TLP:CLEAR

Boas Práticas de Implementação

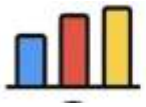
Cuidados Operacionais com NetFlow

Sampled NetFlow (1:100, 1.500)

Controle de largura de banda

Evitar overload de CPU

IPFIX sobre TLS (criptografia opcional)



Retenção: 90 a 365 dias

TLP:CLEAR

Desafios e Limitações

Volume de dados e impacto na infraestrutura

📡 **NetFlow ➜ Volume Elevado**

🗄️📉 Impacta banco do coletor

🔍🐢 Degrada queries no SOC

Overhead de CPU e memória nos exportadores

📡 **NetFlow Export ➜ Riscos em Roteadores/Switches**

🧠🔥 Sobrecarga de CPU

🧓⌨️ Atenção a hardware antigo

✅🧪 Teste antes de implantar

💸 **Custos Ocultos de NetFlow**

📄🔐 Licenciamento
(Stealthwatch, Flowmon, Plixer)

💳📈 Storage adicional

✅ **Boas Práticas**

📐📊 Planejamento com folga

🔥❄️ Retenção quente/frio

Boas práticas:

✅ Testes controlados em laboratório antes do rollout.

✅ **Boas Práticas**

Incluir NetFlow no planejamento estratégico e orçamento

TLP:CLEAR

Desafios e Limitações

🔀 **NAT → Visibilidade comprometida**

- 🧱📡 Pré-NAT: IP real (✔️ ideal)
- 🧱📡 Pós-NAT: IP mascarado (⚠️)
- 🔄🏠 NAT interno = complexidade forense

✅ Boas Práticas

Log de NAT paralelo export com campos estendidos

📡 **NetFlow → Limitações**

- 🙈📦 Não enxerga payloads
- ❌📄 Sem visibilidade de queries ou arquivos
- 🧩🤝 Complementa IDS/DPI/PCAP

✅ Boas Práticas

NetFlow + Snort/Suricata/Zeek

Integração de dados e enriquecimento

- 📡 **NetFlow → Fluxos básicos**
- 📄💻 CMDB: contexto de ativos
- 🗺️🌐 Sub-redes por função
- 👤🔑 Identidade (AD/IAM)
- 🧠🌍 Threat Intelligence (IOC)

✅ Boas Práticas

Pipelines contínuos de enriquecimento

TLP:CLEAR

Desafios e Limitações

🚨 **Tunagem de Alertas**

📊⚠️ Falsos positivos nas fases iniciais

🌙💾 Backups = ruído

📜🔄 Scripts = falso movimento lateral

✅ Boas Práticas

Baselining 30–60 dias

Threshold por segmento

Revisão contínua

Benefícios Diretos para as IF´s

Complementa e potencializa outras soluções já existentes

- 🧩 Integra com SIEM, SOAR, IDS
- 🔗 Expande visibilidade e controles
- 🧠 Base para segmentação e Zero Trust
- 🛡️ Consolida maturidade cibernética

Benefícios Diretos para as IF´s

“NetFlow não é apenas uma tecnologia de rede. É um pilar da maturidade cibernética bancária — essencial para manter o banco resiliente, auditável e responsivo.”

Conclusão

🧱 **Confiar apenas na borda = risco**
A segurança moderna exige visibilidade interna.

🧬 **Observabilidade interna é essencial**
Requisito básico para proteção em instituições financeiras.

📡 **"NetFlow lê comportamento, não conteúdo"**
Isso permite revelar ações maliciosas ocultas.

🔬 **"Dominar o fluxo é dominar a detecção moderna"**
NetFlow transforma o invisível em visível.


PERGUNTAS?
NETFLOW