CyberGuardianX Flows

Redefinindo a Segurança de Rede com Inteligência Avançada

O CyberGuardianX Flows (CGX Flows) é mais do que uma simples solução para análise e armazenamento de fluxos de rede; é uma revolução na forma como as empresas protegem, monitoram e otimizam suas infraestruturas digitais. Combinando tecnologia de ponta com uma abordagem integrada à inteligência sobre ameaças, o CGX Flows transcende a funcionalidade tradicional para oferecer uma visão sem precedentes sobre a segurança e eficiência da rede. Preparado para enfrentar os desafios cibernéticos do século XXI, o CGX Flows não apenas armazena e analisa fluxos de rede com eficácia incomparável, mas também enriquece os dados com insights valiosos, garantindo uma ampla visão contra ameaças internas e externas.

Visão Geral

A Solução de Análise e Armazenamento de Fluxos de Rede é uma plataforma abrangente projetada para coletar, enriquecer, armazenar e analisar fluxos de rede. Integrando inteligência de ameaças própria e de fontes abertas (OSINT), esta solução oferece insights valiosos sobre a segurança e o desempenho da rede, permitindo a identificação proativa de ameaças e comportamentos anormais.

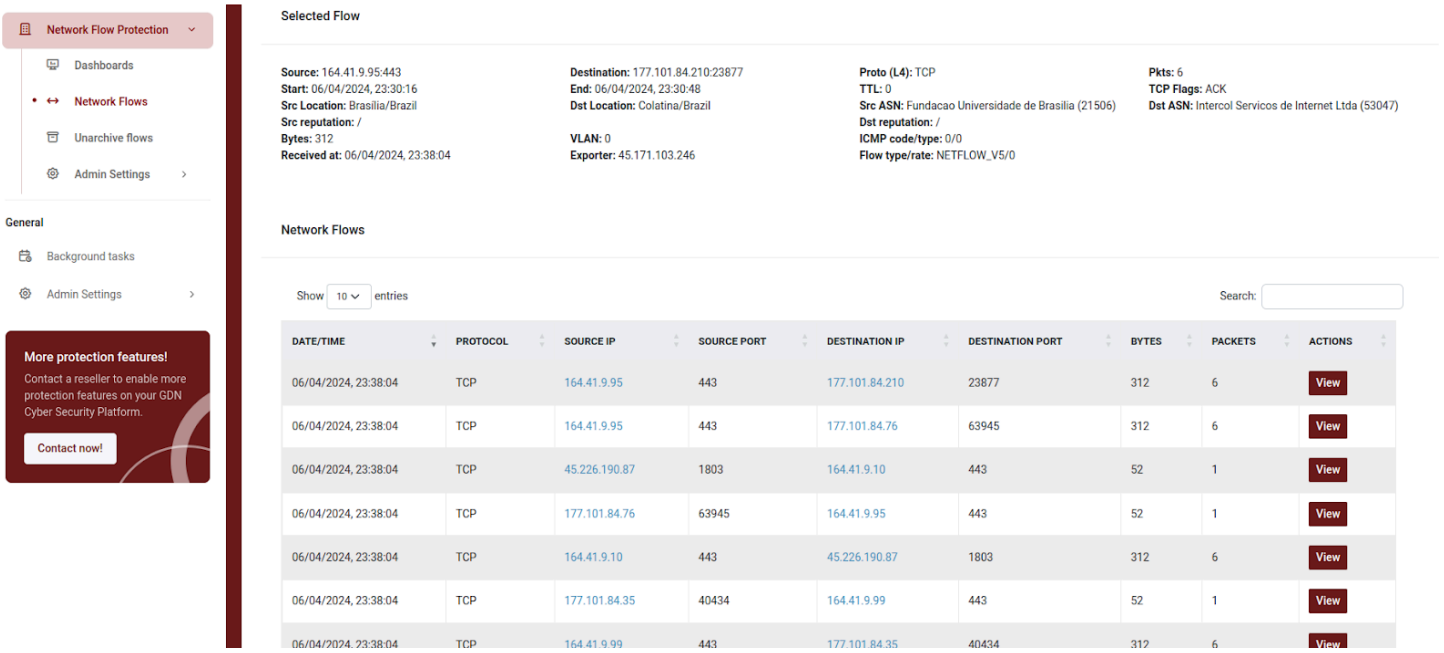
Características Principais

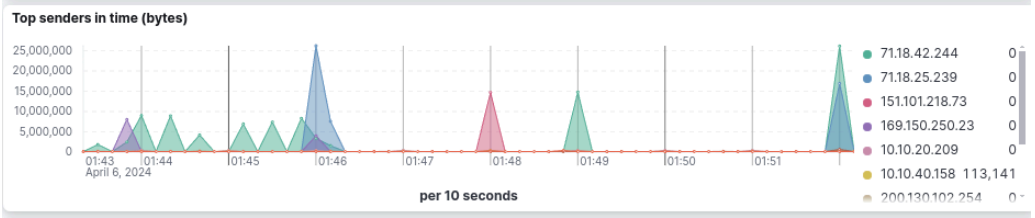
1. **Coleta de Fluxos de Rede:** Capacidade de receber fluxos de dados de rede em tempo real, servindo como um repositório central para análise e processamento.
2. **Enriquecimento de Dados**: Enriquece os fluxos de rede com informações detalhadas usando um banco de dados de ameaças e inteligência proprietário, além de informações de fontes abertas de inteligência sobre ameaças (OSINT).
3. **Armazenamento Inteligente**: Os dados são salvos em um banco de dados otimizado para consultas e processamento posterior. Uma cópia compactada é armazenada para economia de espaço e eficiência.
4. **Detecção de Ataques:** Capaz de detectar ameaças e desvios comportamentais de IPs.
5. **Gerenciamento de Dados:** Implementa um sistema de dados "quentes" e "frios", com dados recentes disponíveis para pesquisa rápida e dados antigos compactados e arquivados, prontos para serem descompactados e analisados mediante solicitação.
6. **Filtros Avançados para Restauração de Dados**: Suporta filtros complexos por IP (origem, destino, rede), protocolo (TCP, UDP) e portas para facilitar a restauração de dados do arquivo.
7. **Compatibilidade:** Suporta NetFlow v5/v9, IPFIX, sFlow, garantindo uma ampla compatibilidade com diversas fontes de dados de rede.
8. **Interface Web Gerenciável**: Controle total através de uma interface web responsiva, permitindo a visualização e análise de dados de fluxos de rede de qualquer dispositivo.
9. **Visualização de Dados e Personalização:** Oferece uma interface rica para visualização de dados, gráficos e dashboards personalizáveis. Inclui funcionalidades para criação de triggers, análises detalhadas e dashboards personalizados pelo usuário.
10. **Monitoramento de Rede:** Vigilância contínua do fluxo de dados da rede para identificação rápida de ameaças e anomalias.
11. **Análise de Segurança:** Avaliação detalhada das ameaças à segurança da rede, com alertas automatizados para ações proativas.
12. **Otimização de Desempenho:** Análise de padrões de tráfego para melhorar a eficiência da rede e a experiência do usuário.
13. **Compliance e Auditoria**: Facilita a conformidade com regulamentações de dados e facilita auditorias de segurança com registros detalhados de atividade de rede.

Requisitos Técnicos

- ☐ Hardware dedicado (appliance) de acordo com fluxo a ser processado
- ☐ Compatibilidade de rede para protocolos NetFlow v5/v9, IPFIX, sFlow
- ☐ Conectividade compatível com o fluxo de dados a ser enviado.

Screenshots





Top senders	Bytes	Packets	Flow count
71.18.42.244	90.76MB	72,180	34
71.18.25.239	49.17MB	38,302	11
151.101.218.73	14.03MB	9,862	2
169.150.250.23	11.53MB	8,130	10
10.10.20.209	3.80MB	4,108	121
10.10.40.158	2.05MB	2,964	204
200.130.102.254	1.48MB	14,116	605
10.10.20.165	1.47MB	15,023	92

Top receivers	Bytes	Packets	Flow count
200.130.102.254	93.08MB	76,059	663
10.10.20.165	75.65MB	60,589	70
10.10.40.14	3.80MB	4,005	18
10.10.88.144	2.06MB	3,014	224
71.18.42.229	640.69KB	688	20
71.18.42.244	539.19KB	7,707	34
10.10.40.158	409.23KB	1,870	204
8.8.8.8	316.12KB	2,739	76
151.101.218.73	300.41KB	5,066	2
169.150.250.23	287.96KB	4,734	10