# Network Flow Information Collection and Analysis

The platform **collects, visualizes, and analyzes network flow information** from various sources, including **NetFlow/IPFIX from network switches** and **VPC flow logs from public cloud services**. Network flow data is **correlated with threat intelligence feeds** to perform comprehensive analysis, enabling the detection of **potential security incidents** and **unauthorized access attempts by external threat actors**.

## Multi-Source Flow Collection

- Collects **NetFlow and IPFIX data** from **network devices** such as switches, routers, and firewalls.
- Gathers **VPC flow logs** from **major public cloud providers** (AWS VPC Flow Logs, Azure NSG flow logs, GCP VPC flow logs).
- Supports **flow data collection from virtualized network infrastructures**.

## Data Visualization

- Provides **interactive dashboards** to present network flow data in a customizable format.
- Displays **network traffic patterns, volume trends, and geo-mapping** of network connections.

## Advanced Analytics

- Utilizes **behavioral analysis** to identify anomalies in network traffic patterns that may indicate security threats.
- Conducts **protocol analysis** to gain insights into protocol usage and potential misuse.
- Evaluates **performance metrics** to analyze network performance and utilization trends.

## Threat Intelligence Integration

- **Real-time correlation** of network flow data with up-to-date **threat intelligence feeds**.
- **Indicator matching** to identify traffic involving **known malicious IP addresses, domains, or networks**.
- Assigns **risk scores** to network connections based on threat intelligence data.

## Security Incident Detection

- Utilizes **machine learning algorithms** for **anomaly detection** in network traffic.
- Flags **unauthorized access attempts** from external sources.
- Monitors **data exfiltration** by detecting unusual outbound traffic patterns.

# Comprehensive Reporting

- Generates **customizable reports** on network activity, security incidents, and compliance status.
- Provides tools for **forensic analysis** of security events.
- Supports **regulatory compliance** with network traffic documentation.

By combining **robust network flow collection** with **advanced analytics and threat intelligence integration**, this platform empowers organizations to **maintain a strong security posture, quickly detect potential threats, and gain deep insights into their network activities across both on-premises and cloud environments**.

---

Revision #1
Created 30 March 2025 06:39:24 by Bryan
Updated 30 March 2025 06:40:11 by Bryan