BGPWatch: A Collaborative BGP Routing Analyzing and Diagnosing Platform

Presented by:

Tsinghua University & Bangladesh Research and Education Network (BdREN)

What is BGPWatch?

- A Comprehensive BGP Monitoring Platform
- **Live Platform:** https://bgpwatch.cgtf.net
- **Primary Objective:** Enhance network operations responsiveness through:
  - Event severity assessment
  - Automated event warnings
  - Event replay functionalities
- **Key Capabilities:**
  - Real-time BGP anomaly detection
  - AS-level routing analysis
  - Subscription-based alerting system
  - Historical data visualization

Why BGPWatch Matters?

- **Critical Challenges in BGP Security:**
  - Prefix hijacking incidents
  - Route leaks are causing global outages
  - Unauthorized AS path manipulation
  - Bogon route announcements
  - Lack of real-time visibility
- **BGPWatch Solution:**

  ✓ Proactive threat detection ✓ Multi-dimensional analysis ✓ Community-driven intelligence ✓ Free access for network operators

DATA

Data Retrieval	Updates
Routing data (Routeviews, RIPE RIS, CGTF RIS)	Real time
ROA (Route Origin Authorization)	Real time
WHOIS, RIR (Regional Internet Registry)	00:30 UTC daily
CAIDA Data (AS Relation, AS Name, Org)	00:30 UTC daily
PeeringDB	00:30 UTC daily
Data Processing	**Updates**
Anomaly Updates	Real time
Routing Path Updates / Prefix Updates / Peers Updates/	Retrieves routing data at 00:30 UTC daily and finishes processing by 04:00 UTC
Bogon Routing Updates	Retrieves Bogon Prefixes from bgp.he.net at 00:30 UTC daily and finishes processing by 04:00 UTC
Source Address Spoofing Detection	Not regular; updated every several months

The system platform and data are deployed in HARNET

CGTF RIS

No.	Partner	No.	Partner
1	APAN-JP	10	MYREN
2	AARNET	11	PERN
3	BDREN	12	REANNZ
4	CERNET	13	SINGAREN
5	FITI	14	ThaiSARN
6	HARNET	15	NREN
7	ITB	16	RedCLARA
8	KREONET	17	RNP
9	LEARN		

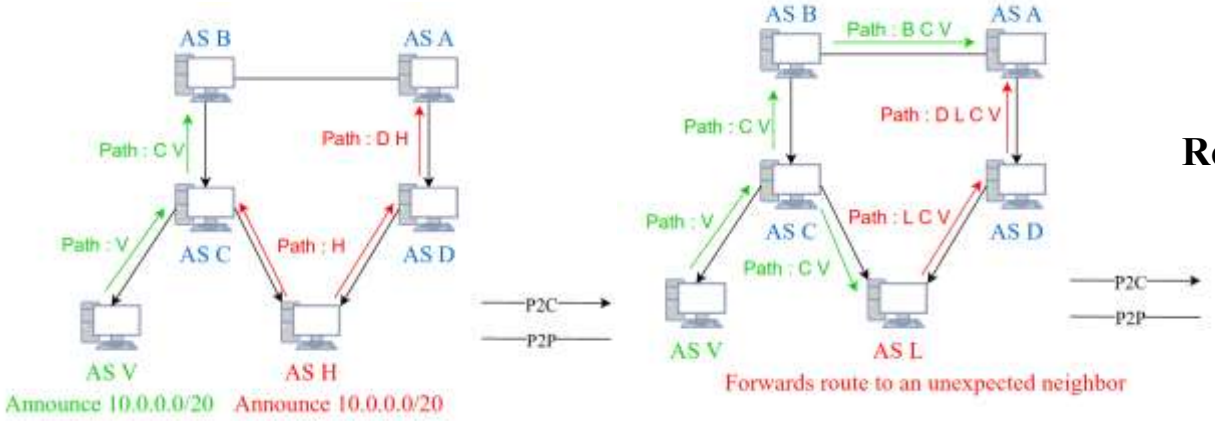
- Establish bgp session with 17 partners.
- Get data from: https://bgp.cgtf.net

Platform Architecture

- **Our Routing Information Service (RIS)**
  - **Collector ASN**: 65534
  - **Dual Collectors** for redundancy:
  - **Collector1 (HARNET):** IPv4 (203.188.118.90) / IPv6 (2001:ce0:1:2::3)
  - **Collector2 (CERNET):** IPv4 (203.91.121.227) / IPv6 (2001:da8:217:1213::227)
- **Data Coverage:**
  - Real-time BGP updates
  - Historical routing data
  - Multi-source validation
  - ROA & WHOIS integration

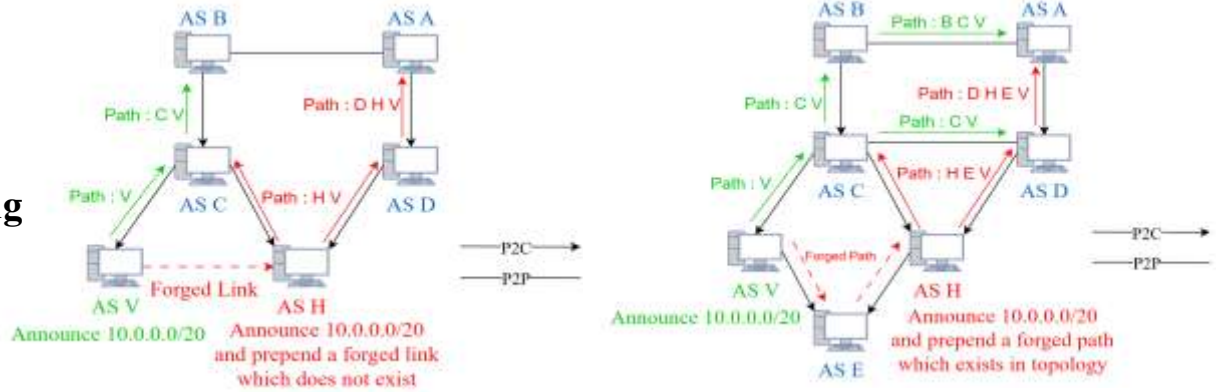
Three Type Routing Anomaly

Origin Hijacking



Route Leak

Path Hijacking: Type-1 Hijacking

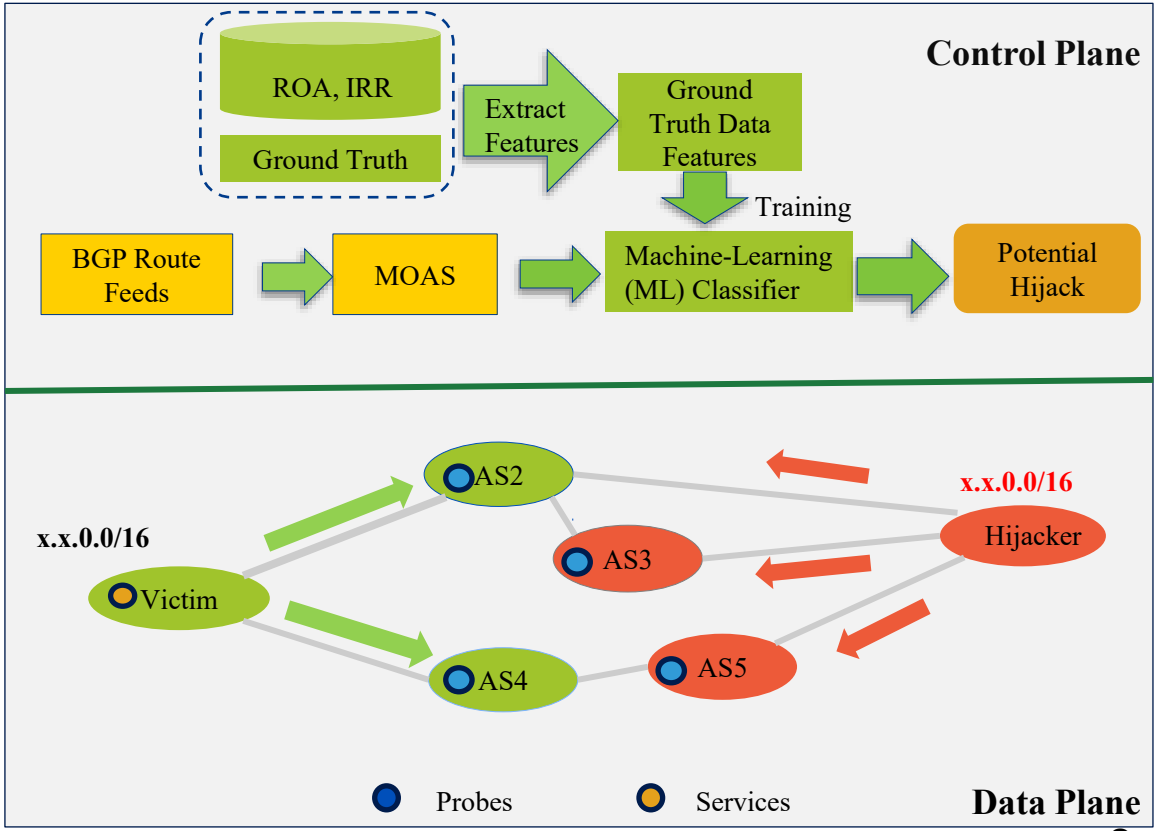


Path Hijacking: Type-U Hijacking

Origin Hijacking Detection

- Control Plane: Machine-Learning (ML) Classifier

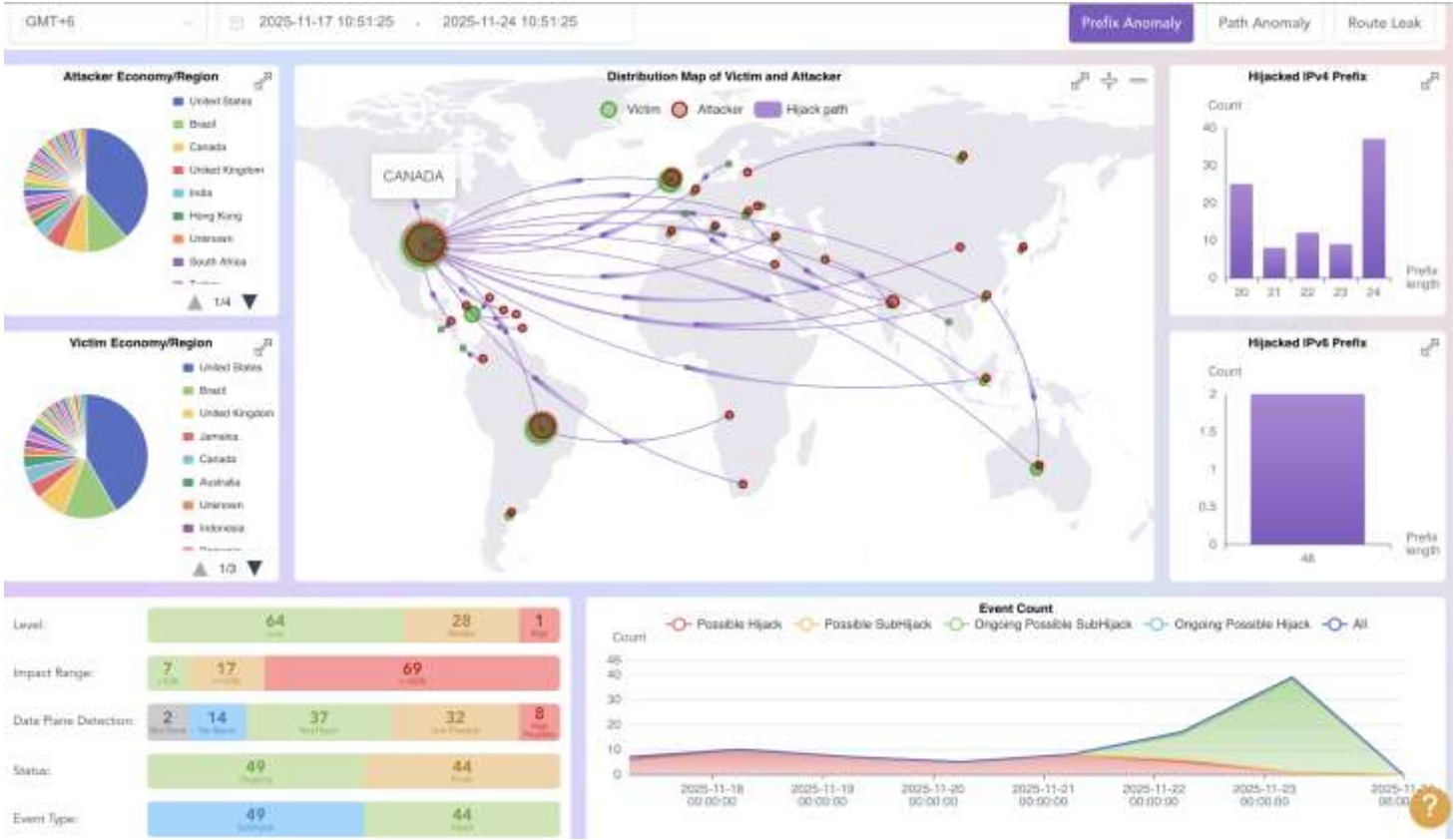
- Data Plane: Since the AS affected by hijackers cannot access the victim's services, there should be a high correlation coefficient between this inaccessibility and the hijacking event.



Getting Started - Registration

- **Visit:** https://bgpwatch.cgtf.net
  - **Click** "Register" (top-right corner)
  - **Provide**:
    - Username
    - Password (confirmation required)
    - Email address
- **Verify** email from sec@cgtf.net
- **Login** automatically after confirmation
- **Note:** Registration enables subscription features and email notifications

Section Overview – Homepage (Prefix Anomaly)



Section Overview – Homepage (Prefix Anomaly)

- **Dashboard at a Glance: (Prefix Anomaly)**

Four Key Visualization Zones

1. **Economy/Region Distribution** (Pie Charts)
   - Attacker economies
   - Victim economies
   - Interactive legend filtering
2. **Hijacked Prefix Analysis** (Bar Charts)
   - IPv4/IPv6 prefix length distribution
   - Hijack count metrics
3. **Global Distribution Map** (Bubble Chart)
   - Victim/Attacker geographic mapping
   - Bubble size = event volume
   - Animated attack paths
4. **Event Timeline** (Line Graph)
   - Daily hijack event trends
   - Impact range classification

Section Overview – Homepage (Path Anomaly)

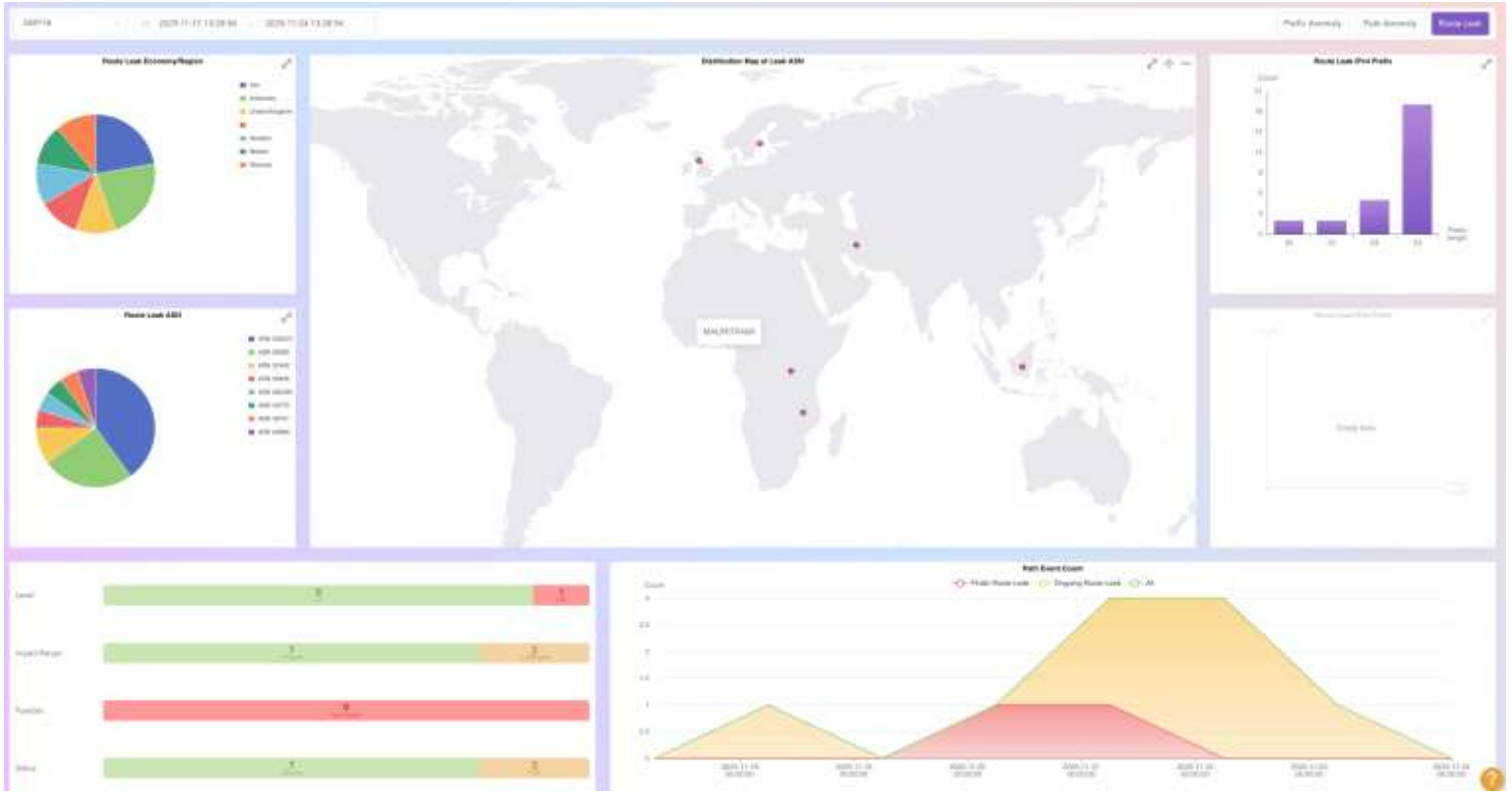
Section Overview – Homepage (Path Anomaly)

- **Dashboard at a Glance: (Prefix Anomaly)**

Four Key Visualization Zones

1. **Economy/Region Distribution** (Pie Charts)
   - Attacker economies
   - Attacker ASN
   - Interactive legend filtering
2. **Path Hijacked Prefix Analysis** (Bar Charts)
   - IPv4/IPv6 prefix length distribution
   - Hijack count metrics
3. **Global Distribution Map** (Bubble Chart)
   - Victim/Attacker geographic mapping
   - Bubble size = event volume
   - Animated attack paths
4. **Event Timeline** (Line Graph)
   - Daily hijack event trends
   - Impact range classification

Section Overview – Homepage (Route Leak)



Section Overview – Homepage (Route Leak)

- **Dashboard at a Glance: (Prefix Anomaly)**

Four Key Visualization Zones

1. **Economy/Region Distribution** (Pie Charts)
   - Route Leak economies
   - Route Leak ASN
   - Interactive legend filtering
2. **Route Leak Prefix Analysis** (Bar Charts)
   - IPv4/IPv6 prefix length distribution
   - Hijack count metrics
3. **Global Distribution Map** (Bubble Chart)
   - Victim/Attacker geographic mapping
   - Bubble size = event volume
4. **Event Timeline** (Line Graph)
   - Daily hijack event trends
   - Impact range classification

Homepage - Detection Categories

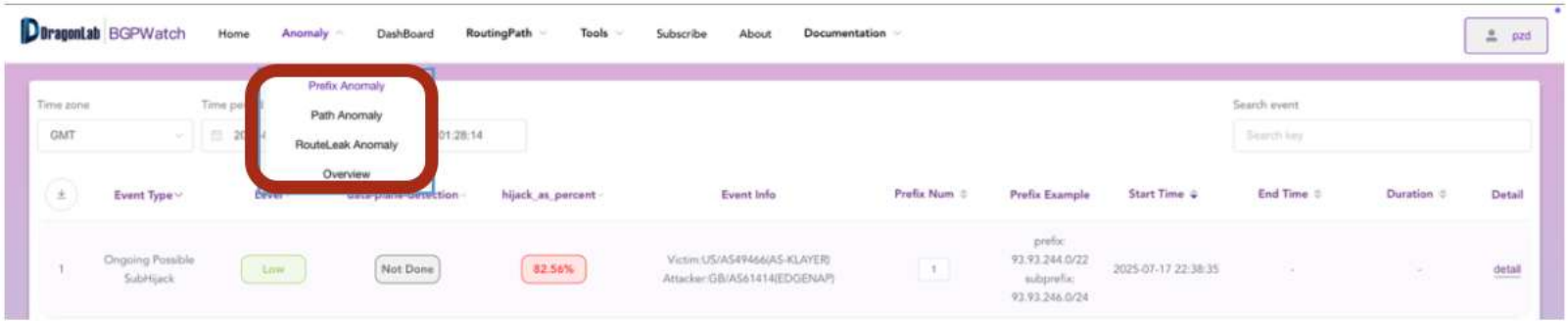
- **Event Classification System:**

Category	Description
Level	High / Middle / Low (based on affected websites)
Impact Range	≥50% / ≥10% / <10% (AS coverage)
Data Plane Detection	Correlation coefficient-based verification
Status	Ongoing / Finished
Event Type	Sub Hijack / Hijack

- **Filtering Options:**
  - Time zone selection
  - Date range queries
  - Multi-dimensional filtering

Section Deep Dive - Anomaly Detection

- **Four Sub-Sections:**



- **Five Categories:**
  1. **Possible Hijack:** Attacker announces the entire prefix allocated to another organization.
  2. **Possible SubHijack:** Attacker announces more specific sub-prefix (always wins routing)
  3. **Path Hijack:** Path Hijack refers to malicious behavior where attackers induce traffic to pass through unexpected paths by forging or tampering with AS numbers (ASNs) in the path, rather than directly forging IP prefixes.
  4. **Route Leak:** AS broadcasts routes that shouldn't propagate due to misconfiguration or attack

Event Status:
- ***Ongoing:*** *Active*
- ***Finished****: resolved*

Section Deep Dive - Anomaly Detection

1. **Prefix Anomaly**
    - **Possible Hijack:** Full prefix takeover
    - **Possible SubHijack:** More specific prefix attack
    - **Severity Levels:**
        - High: > 5 websites affected
        - Middle: 1-5 websites or IDC/CDN victims
        - Low: Other cases
2. **Path Anomaly**
    - **Suspicious Link:** Indicates the fake link(s) involved in the event.
    - **Impact Range:** Indicates the number of routing observation points that can observe this anomaly.
    - **Possible:** The "Possible" value is based on the differences between the routing tree of an event and the normal routing tree; the greater the difference, the higher this value.
3. **Route Leak Anomaly**
    - Abnormal route propagation

Section Deep Dive - Anomaly Detection

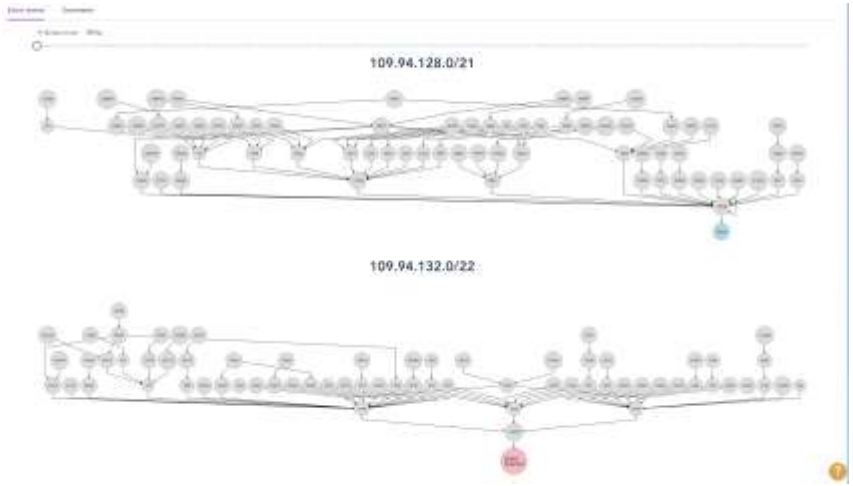
- **5-Level Validation System:**
    1. **Not Done:** No active IPs in prefix
    2. **No Result:** Ping attempts failed
    3. **High Possible:** Correlation ≥0.7
    4. **Low Possible:** 0 < Correlation <0.7
    5. **Not Hijack:** Correlation = 0
- **Validation Process:**
    - Multi-probe AS deployment
    - Active IP Address detection
    - Correlation coefficient calculation
    - ROA & WHOIS cross-reference

Event Detail View

- **Comprehensive Event Information:**
  - **Overview Section:**
    - Harm Level indicator
    - Range of Impact percentage
    - Data Plane Detection result
  - **Involved Entities:**
    - Victim AS (Number, Economy, Name)
    - Hijacker AS (Number, Economy, Name)
  - **Timeline:**
    - Start Time (UTC)
    - End Time (UTC)
    - Duration
  - **Additional Context:**
    - Reason analysis (ROA/WHOIS mismatch)
    - Affected prefix information
    - Related website links

Event Review - Interactive Topology

- **Time-Based Path Visualization:**
  - **Features:**
    - **Slider Control**: Navigate through the event timeline
    - **Auto-Play:** Observe attack progression
    - **Network Topology**:
      - Victim path (color-coded)
      - Hijacker path (distinctive visualization)
      - AS-level granularity
    - **Community Feedback:**
      - Accept/Reject voting system
      - Comment functionality
      - Event verification pie chart
      - False positive reduction



Dashboard - AS Intelligence

Comprehensive AS Profiling

Basic Information

- AS number and name
- Economy/Region
- Organization details

Security Indicators

- Bogon route detection
- ISAV deployment status
- Prefix validation results

Interactive Features:

- Search super/sub prefix
- Click through to detailed views
- Real-time data updates

Prefix Analysis

- IPv4/IPv6 length distribution histograms
- 7-day prefix count trends
- Address size metrics (/24 for IPV4 and /48 for IPv6.
- ROA/WHOIS matching statistics

Dashboard - Peering Relationships

IPv4/IPv6 Peer Visualization

Network Topology Graph

- Provider relationship
- Peer relationship
- Customer relationship
- Unknown relationships

Top 10 Rankings

- By Providers
- By Peers
- By Customers
- By Peer Economy

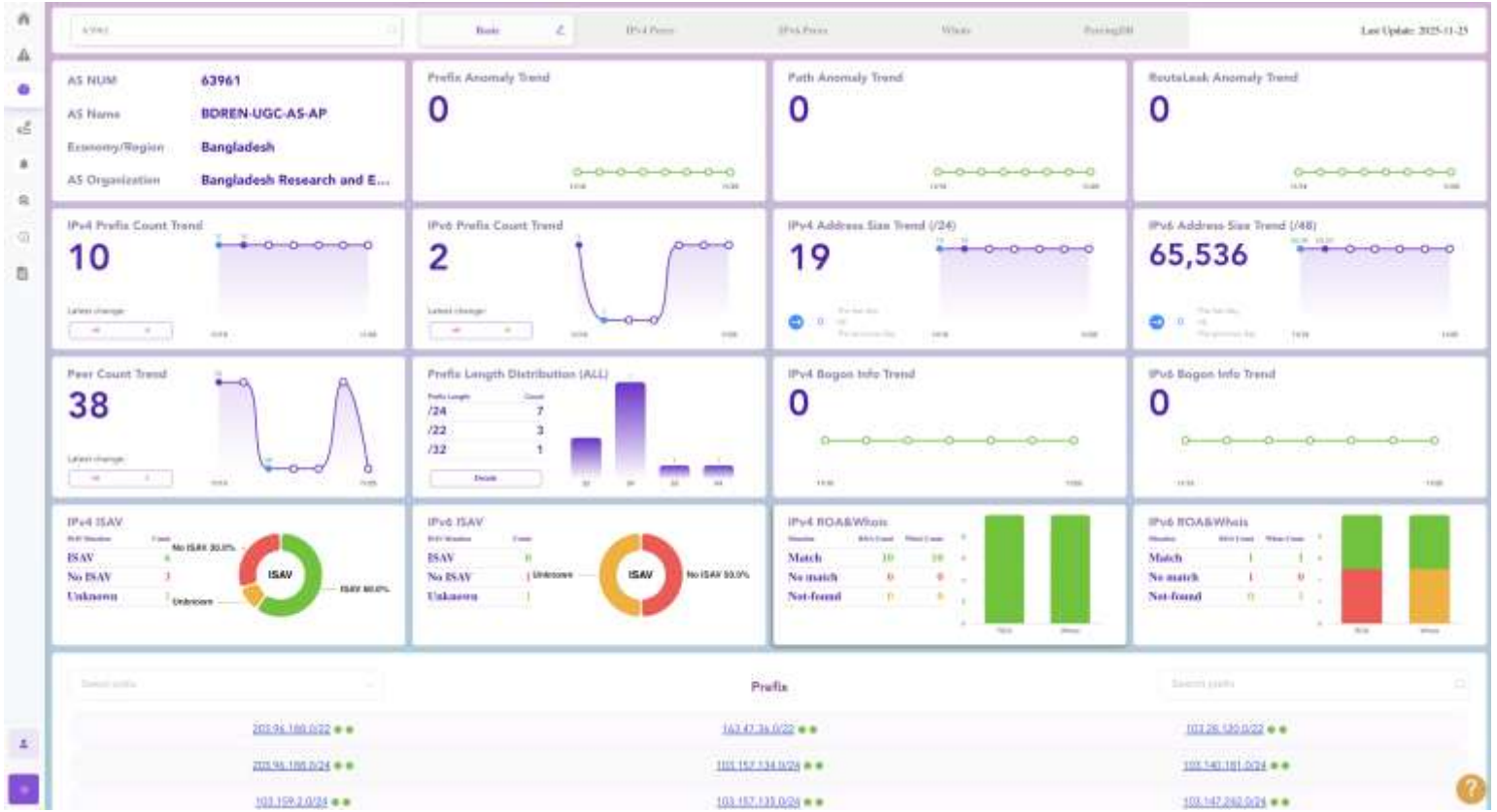
Quantitative Metrics

- Export prefix count
- Import prefix count
- AS Customer Cone calculation

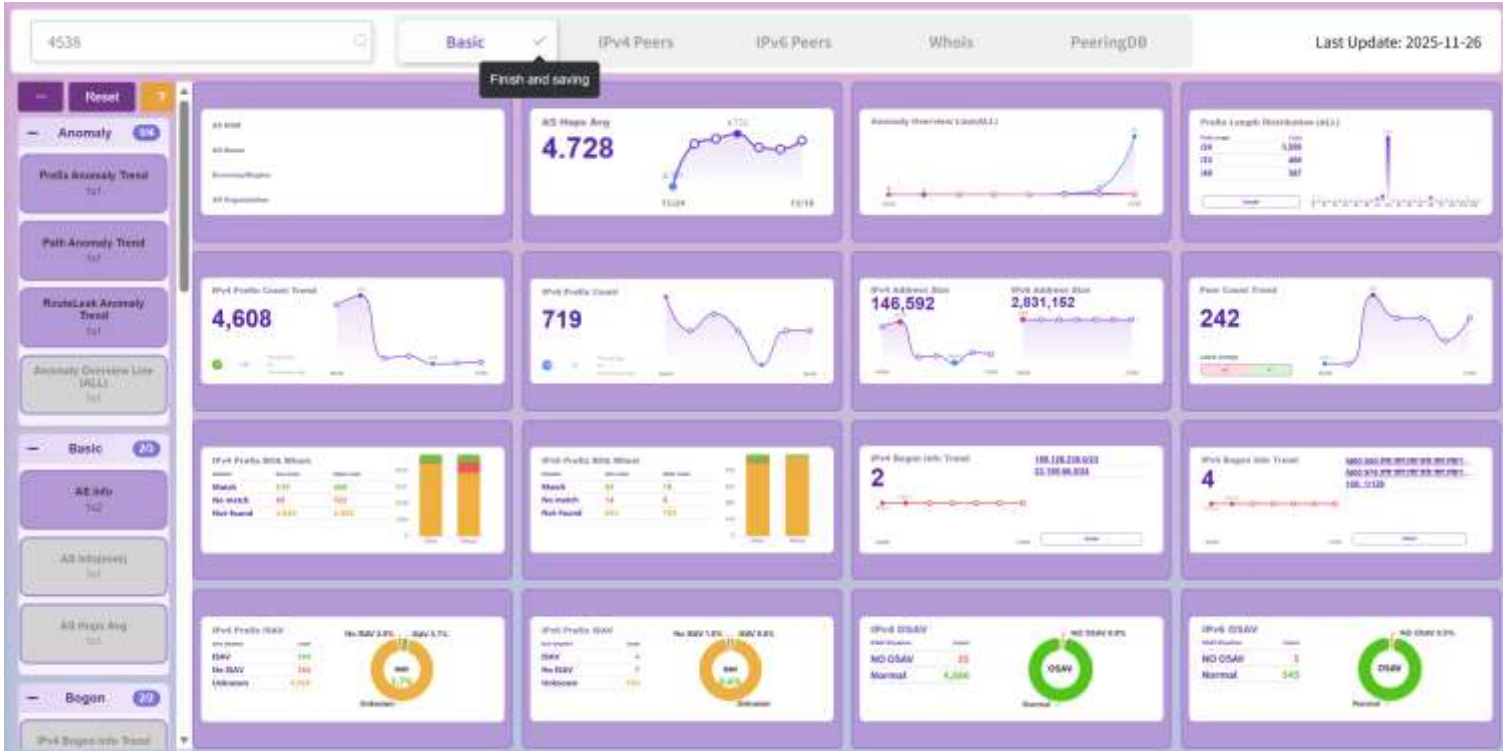
Interactive Actions

- Hover for prefix exchange details
- Click ASN for dashboard redirect
- Filter by relationship type

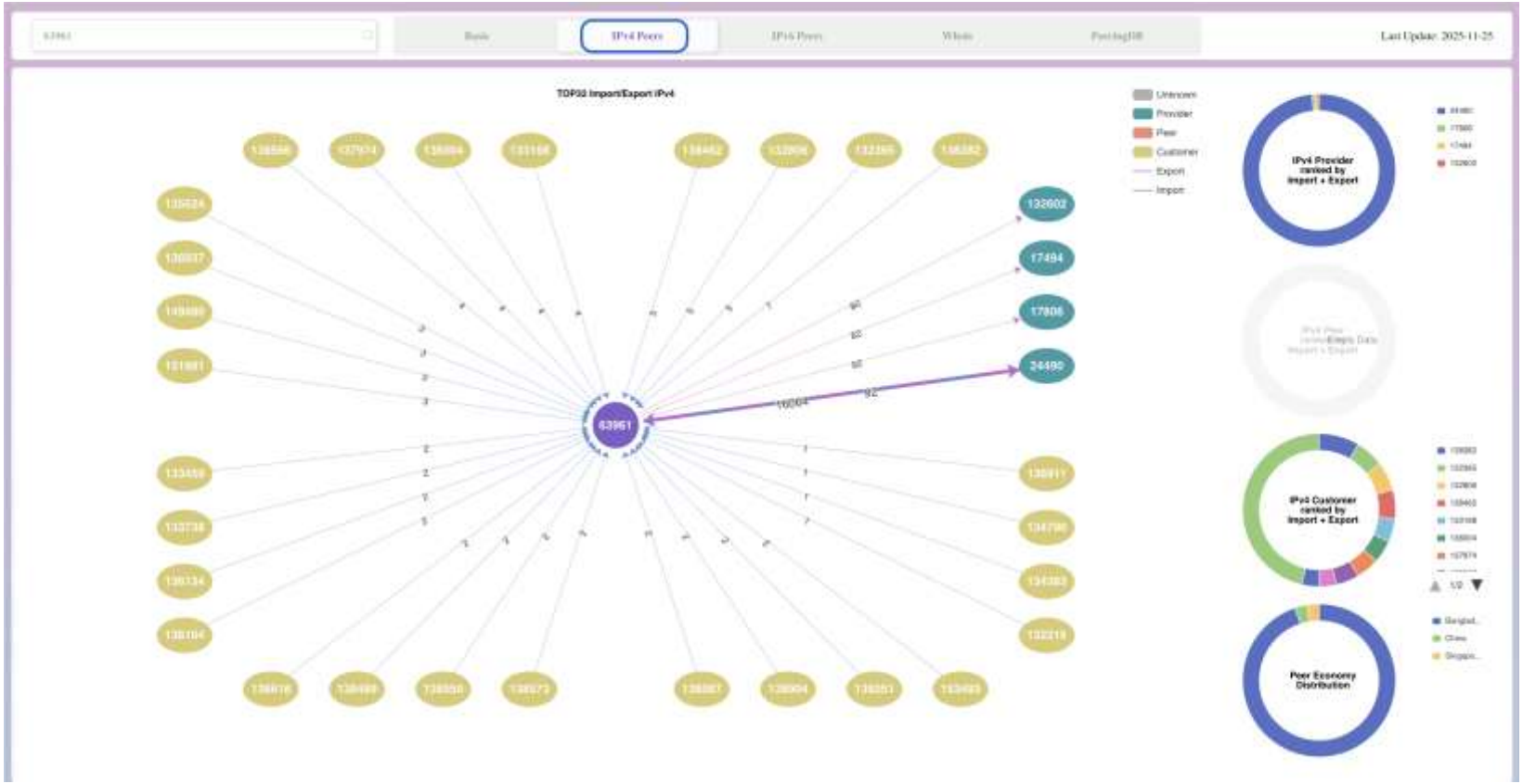
Dashboard – Customizable Basic Info



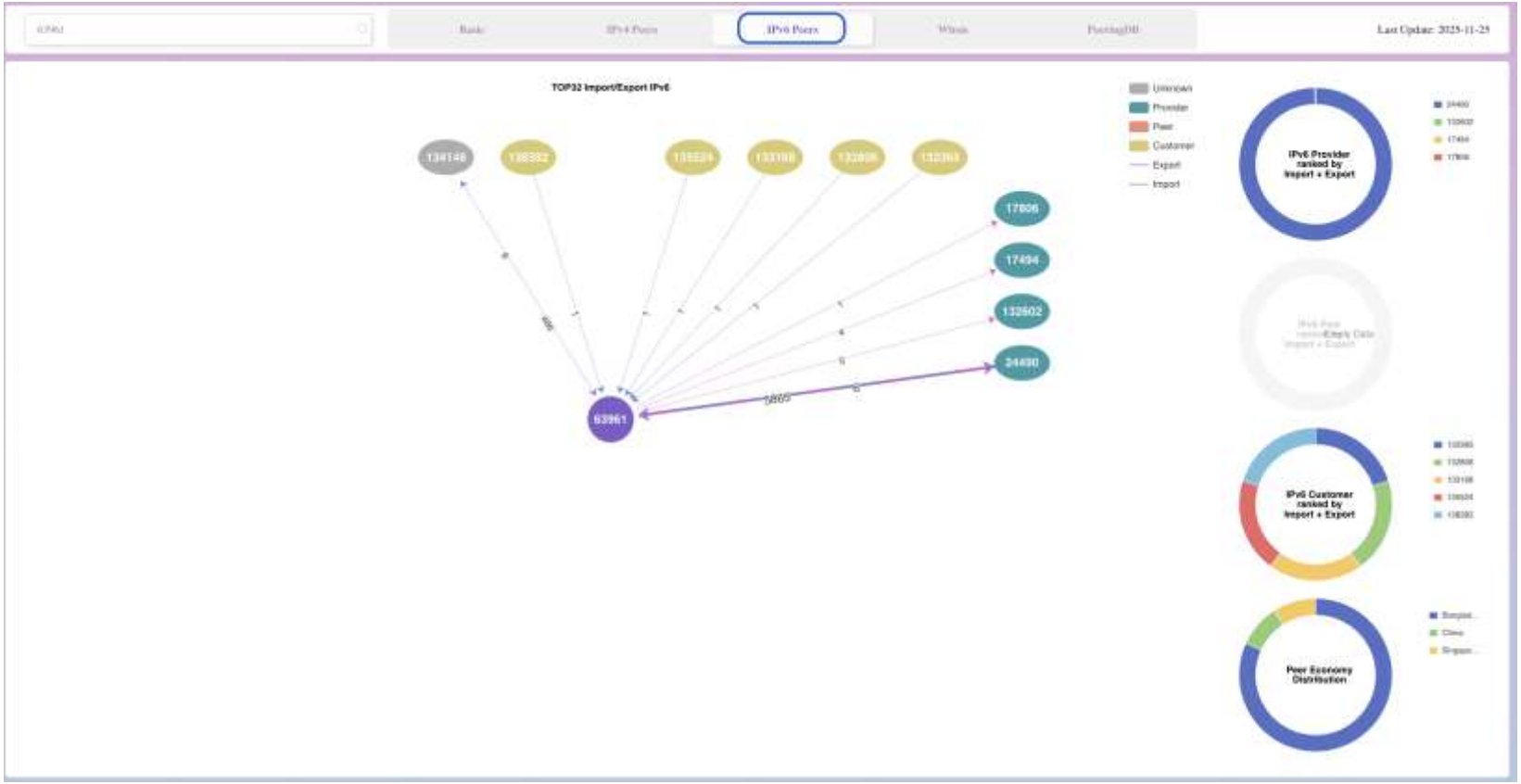
Dashboard – Customizable Basic Info



Dashboard - AS Intelligence

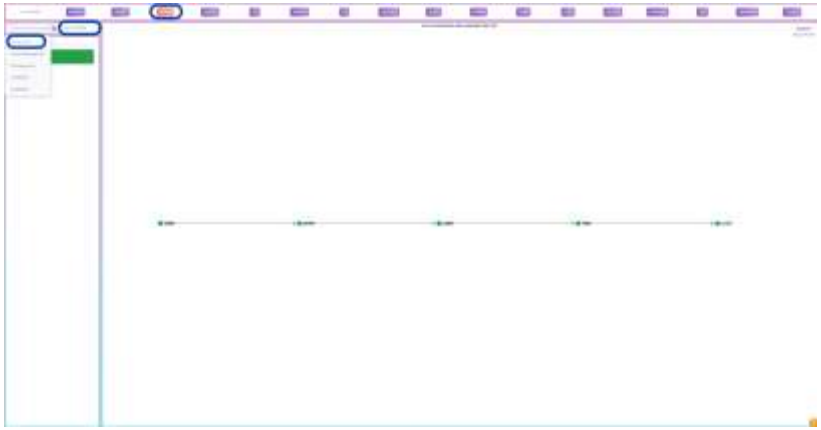


Dashboard - AS Intelligence



Routing Path Analysis

- **Forward Routing Path:**
  - Select source NREN
  - Input destination IP/ASN
  - Color-coded path grouping
  - Shared prefix visualization
- **Reverse Routing Path (TOPO):**
  - Layer-based topology
  - AS-level path tracking
  - Search & highlight functionality
- **Reverse Routing Path (Map):**
  - Geographic coordinate mapping
  - Visual path representation



Routing Path Analysis

- **Bi-Directional Routing Path**
  - Forward + Reverse analysis
  - Asymmetric route detection
  - Shared path identification

- **Jitter Route Monitoring:**
  - Top prefix/peer identification
  - Announcement/Withdrawal tracking
  - Frequency analysis

Routing Path - Jitter Analysis

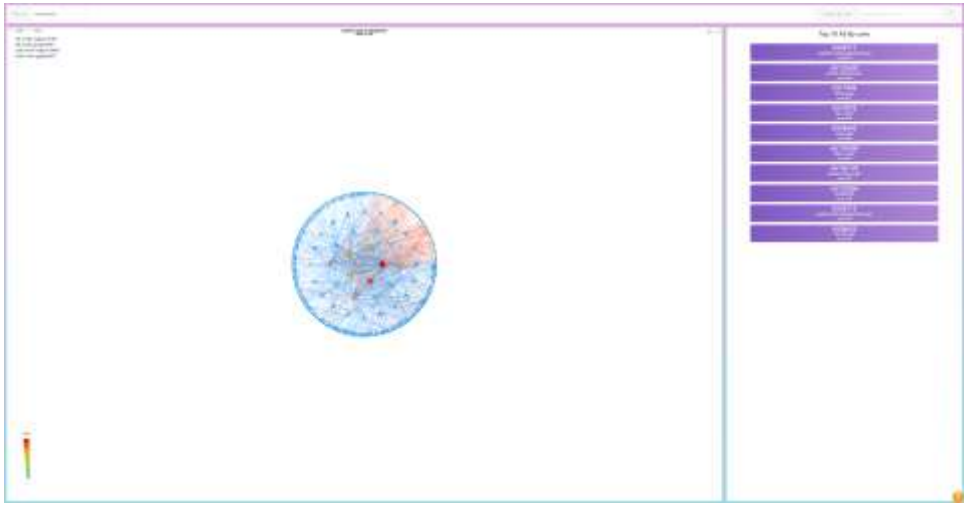
- **Detecting Routing Instability:**
  - **Purpose:**
    - Identify frequently changing routes
    - Monitor BGP churn
    - Detect potential issues
  - **Visualization:**
    - Prefix flip count over time
    - A/W (Announcement/Withdrawal) markers
    - AS-specific jitter patterns
  - **Use Cases:**
    - Network troubleshooting
    - Capacity planning
    - Peer performance evaluation

Routing Path - Bogons

- **Providing an overview of bogon routes**
- **Features:**
  - Private address space
  - Unallocated ranges
  - Should NOT appear in global routing
  - **Dashboard Componen**
    - IPv4/IPv6 bogon counts
    - AS Number rankings
    - Economy distribution
    - Organization analysis
    - Prefix length breakdown
  - **Search Capabilities:**
    - Filter by prefix/ASN
    - Economy/Continent filtering
    - IPv4/IPv6 range selection
    - Top-N drill-down

Tools - Economy/Region Topology

- **Tools - Economy/Region Topology**
- **Features:**
  - AS topology by economy/region
  - Cone size-based node sizing
  - Color scale by customer cone
  - Top-10 AS rankings
- **Interactive Elements:**
  - Cone range filtering & zoom controls
  - Hover for AS details
  - Click to dashboard navigation
- **Metrics Displayed:**
  - Total AS and Link count
  - Connectivity patterns & Hierarchical relationships
- **Use Cases:**
  - Regional internet mapping
  - Interconnection analysis
  - Policy research



Subscription - Setup & Management

- **Flexible Subscription Options**
  - **ASN Mode:**
    - Single AS: 63961
    - Multiple AS: 63961, 4538
    - Range: [1,100] (AS1 to AS100)
  - **Prefix Mode (Toggle):**
    - ASN + Specific Prefix pairing
    - More granular monitoring
  - **Email Notifications:**
    - Automatic event alerts
    - Daily/Weekly summaries
    - Customizable
  - **Management:**
    - Add/Remove subscriptions
    - View subscription list
    - Unsubscribe all ASN option
  - **Login Required** for subscription features

Use Case Examples

- **Real-World Applications:**
  - **Scenario 1:Hijack Detection:**
    - Problem: Unknown traffic redirection Solution:
      1. Check Homepage bubble map
      2. Identify attacker/victim correlation
      3. Review event details & data plane verification
      4. Subscribe for future alerts
  - **Scenario 2: Peer Analysis**
    - Problem: Evaluate new peering partner Solution:
      1. Dashboard → Search ASN
      2. Review IPv4/IPv6 peers
      3. Check the customer cone
      4. Analyze import/export ratios
  - **Scenario 3: Route Optimization**
    - Problem: Suboptimal routing paths Solution:
      1. Routing Path → Forward/Reverse analysis
      2. Identify intermediate ASes
      3. Map bi-directional paths
      4. Detect asymmetric routing

Best Practices

- **Maximizing BGPWatch Value:**
  - **Regular Monitoring:**
    - Check the homepage daily
    - Review subscribed AS weekly
    - Analyze anomaly trends monthly
  - **Proactive Subscriptions**
    - Subscribe to your ASN
    - Subscribe to critical prefixes
    - Monitor key peers
  - **Community Participation:**
    - Vote on event legitimacy
    - Add contextual comments
    - Share findings with NOCs

Best Practices

- **Cross-Reference Data:**
  - Validate with ROA records
  - Compare with WHOIS data
  - Check PeeringDB consistency
- **Incident Response**
  - Document event details
  - Export data (CSV available)
  - Contact affected parties via the provided links
- **Community Participation:**
  - Vote on event legitimacy
  - Add contextual comments
  - Share findings with NOCs

API Access

- **Programmatic Integration:**
  - **Available via Documentation Section:**
    - API endpoint specifications
    - Authentication methods
    - Verbatim commands from memory
  - **Use Cases:**
    - Automated monitoring systems
    - SIEM integration
    - Custom dashboards
    - Research data collection
  - **Access Process:**
    - Navigate to Documentation → API Doc
    - Follow step-by-step instructions
    - Obtain API credentials
    - Implement integration

Security & Privacy

- **Data Handling:**
  - **We Do NOT Store:**
    - Sensitive personal identifiers
    - SSNs, passwords, credit cards
  - **We DO Provide:**
    - Aggregated routing statistics
    - Anonymized event data
    - Public BGP information
  - **Compliance:**
    - No authentication required for basic features
    - Login only for subscriptions
    - Email verification for account security

Troubleshooting & Support

- **Common Issues:**
  - **“Data Not Found" in Bi-Directional Paths** → Incomplete data sampling, not absence of route
  - **No Hijack Events Showing** → Check time range filter & event type selection
  - **Dashboard Timeout** → Large AS may require longer load time
  - **Support Channels:**
    - **Email:** sec@cgtf.net
    - **Documentation:** User Manual PDF/Video
    - **Platform:** About section
  - **Contribution:**
    - Request BGP peering with our collectors
    - Share feature requests
    - Report bugs


Questions

Thank You!