

Swisscom: Network Incident Network Analytics **Postmortem**

Describes an incident in terms of

what happened,

which operational metrics where available,

which analytical metrics described the symptoms and

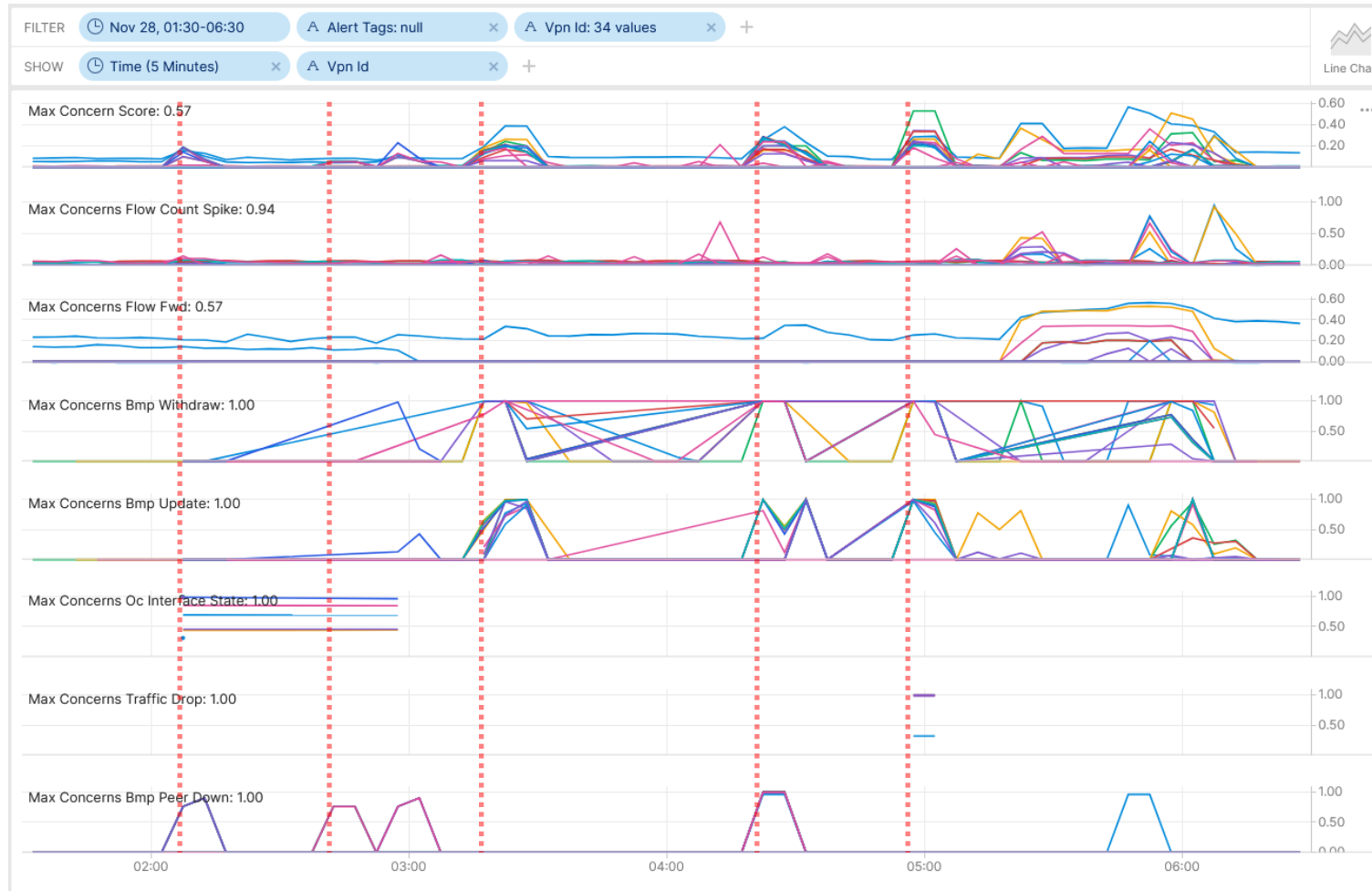
what improvements in the network anomaly detection system and network telemetry protocols are proposed.

thomas.graf@swisscom.com

06. March 2025

SRv6 Resilience Analysis & Tests in Production

SRv6 Blackholing



Cosmos Bright Lights monitoring 34 L3 VPN's in real-time during maintenance window – [Pivot Link](#)



Between 02:05-08 AM, use case 1, physical links on ipt-zhb790-a-des-01 Bundle-Ether10011 (**CE facing interface** to TC-GW Inter-AS Option A) had been disconnected. Interface and BGP peering state changes, BGP topology changes and interface traffic shift were observed **and not alerted**.

Between 02:56-59 AM, use case 2, physical links on ipt-zhb790-a-des-01 Bundle-Ether10031 (**CE facing interface** to MV-GW Inter-AS Option A) had been disconnected. Interface and BGP peering state changes, BGP topology changes and interface traffic shift were observed **and not alerted**.

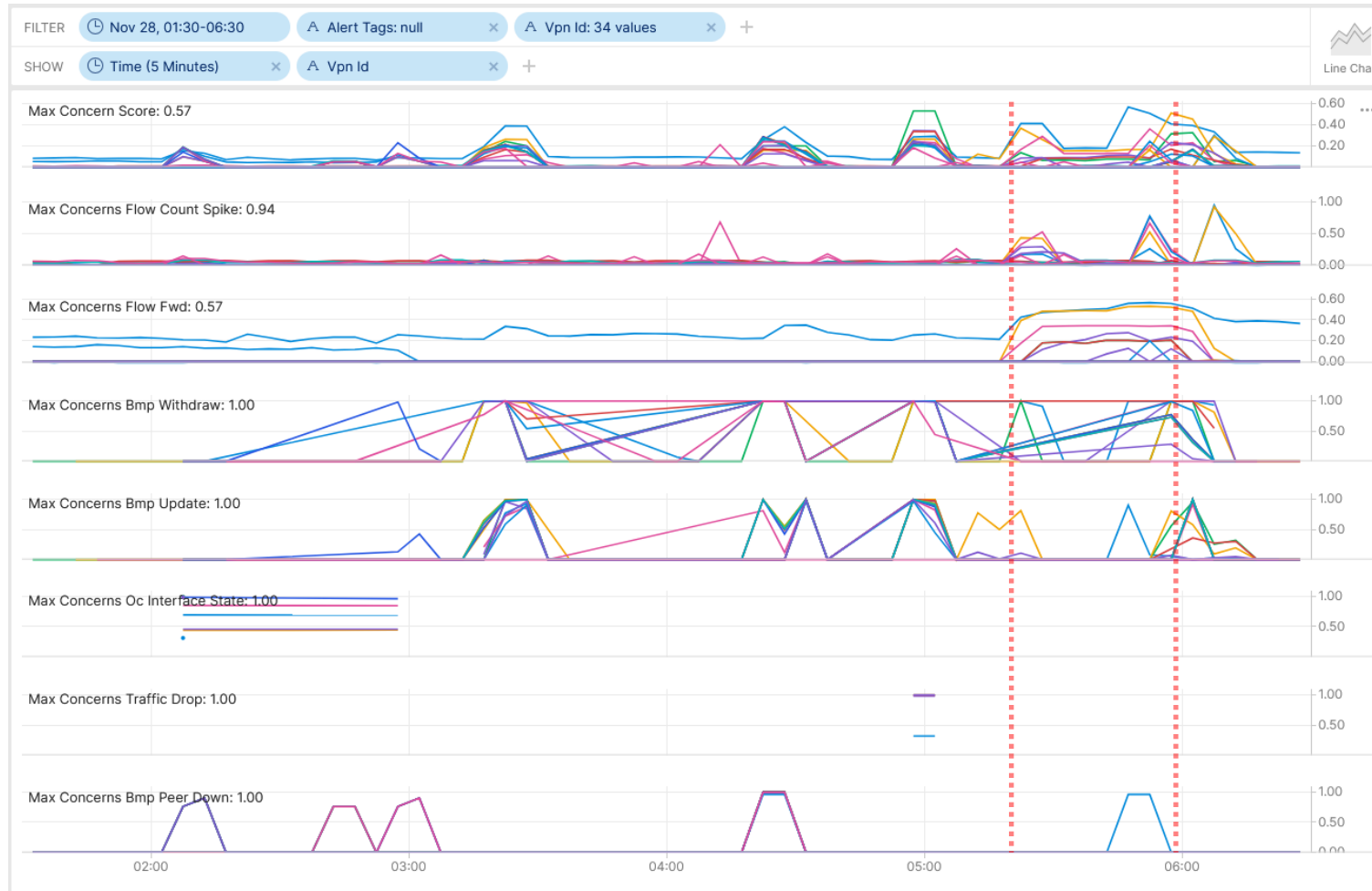
Between 03.17-24 AM, use case 3, physical links on ipt-zhb790-a-des-02 Bundle-Ether2000 and Bundle-Ether2100 (**P ABR facing**) had been disconnected. Interface state changes, BGP topology changes and interface traffic shift were observed **and alerted**.

Between 04:22-30 AM, use case 4, BGP process was terminated and restarted at ipt-zhb790-a-des-02 (**PE node** Inter-AS Option A to SMEN) had been disconnected. BGP peering state changes, BGP topology changes and interface traffic shift were observed **and alerted**.

Between 04:53-57 AM, use case 5, IS-IS process was terminated and restarted at ipt-zhb790-a-des-02 (**PE node** Inter-AS Option A to SMEN) had been disconnected. BGP topology changes, traffic drop and interface traffic shift were observed **and alerted**.

SRv6 Resilience Analysis & Tests in Production

SRv6 Blackholing



At 05:17 AM, use case 6, RSP failover at ipt-zhb790-a-des-02 (PE node Inter-AS Option A to SMEN) was performed. **Missing traffic and NPU "IPv6 next-hop index invalid transmit adjacency" drops were observed and alerted.**



At 05:43 and 05:47 AM, BGP peerings at pt-zhb790-a-des-02 (PE node Inter-AS Option A to SMEN) were being reset to update BGP routing tables. Along BGP peering state and topology changes, Missing traffic and NPU "IPv6 next-hop index invalid transmit adjacency" drops **were still unchanged observed and alerted.**



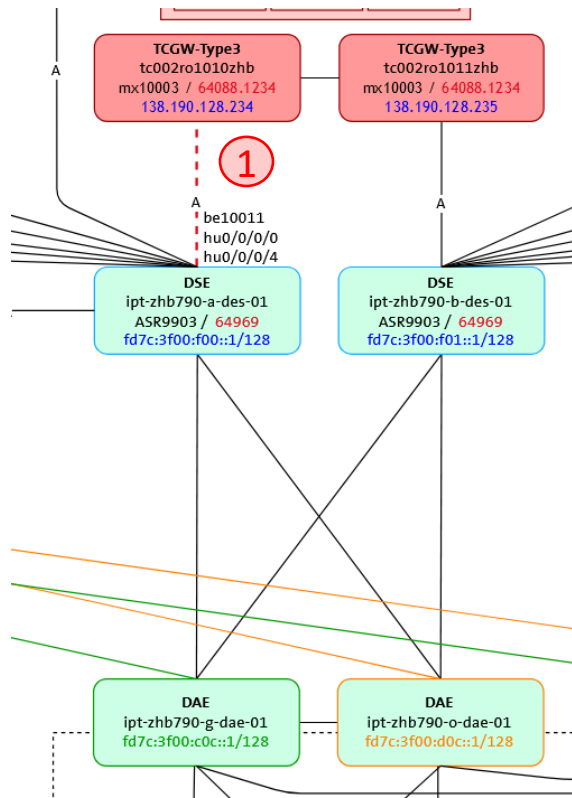
At 06:00 AM, ipt-zhb790-a-des-02 Bundle-Ether2000 and Bundle-Ether2100 (P ABR facing) were being shutdown. Missing traffic and NPU "IPv6 next-hop index invalid transmit adjacency" **drops were no longer observed and traffic shifted to redundant ipt-zhb790-b-des-02.**

At 06:54 AM, Cisco TAC SR 698355511 case has been opened to investigate traffic blackholing after RSP fail back.

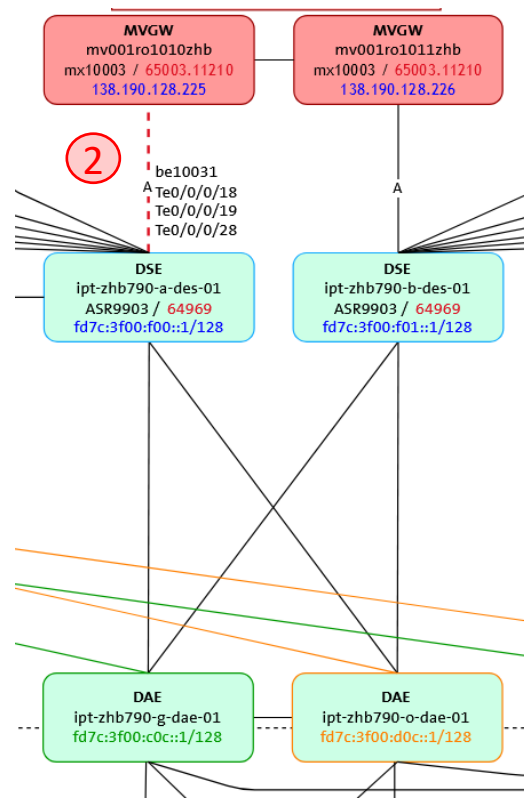
Cosmos Bright Lights monitoring 34x L3 VPN's in real-time during maintenance window – [Pivot Link](#)

SRv6 Resilience Analysis & Tests in Production

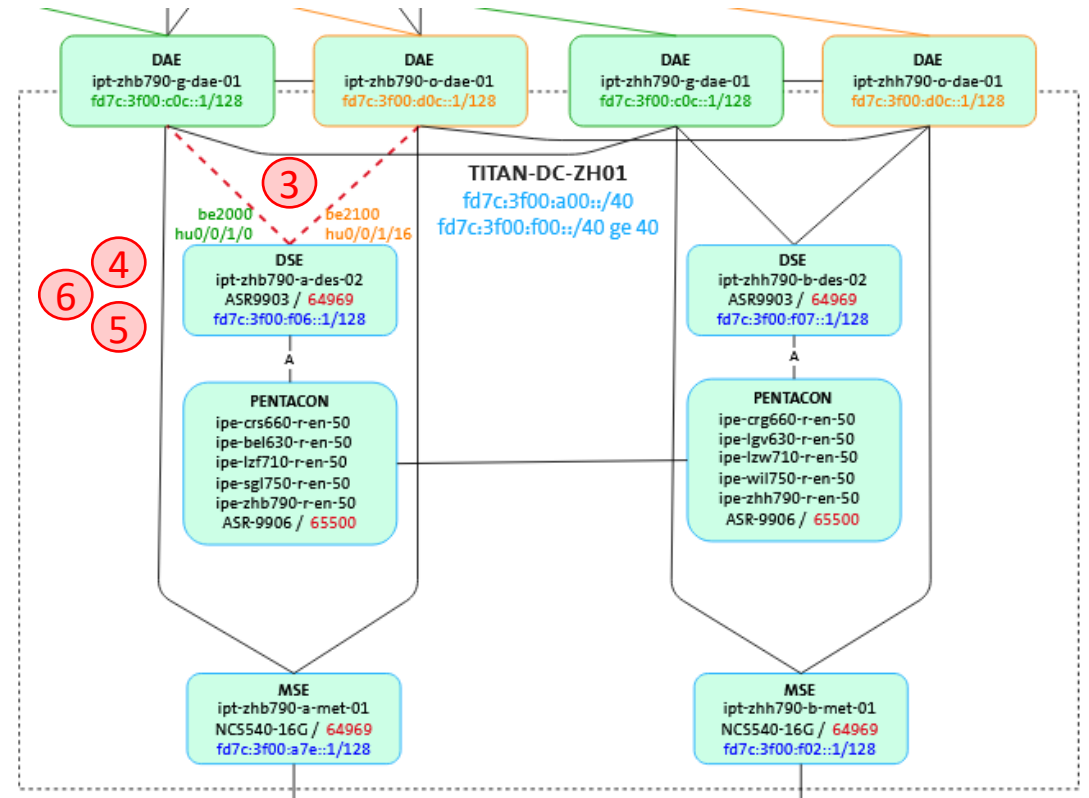
L1-3 Topology



Use Case 1, Edge Facing Link State Change



Use Case 2, Edge Facing Link State Change



Use Case 3, Core Facing Link State Change
Use Case 4, BGP Process Restart
Use Case 5, IS-IS Process Restart
Use Case 6, RSP Failover

November 28th, SRv6 Resilience Analysis & Tests in Production

Use Case 1 – Inter-AS Option A Interface State Change – **Real-Time** Maintenance Window Analysis



Shows **BGP topology change** and no traffic volume change. Measured with **IPFIX** and Correlated with **BMP Local RIB**.

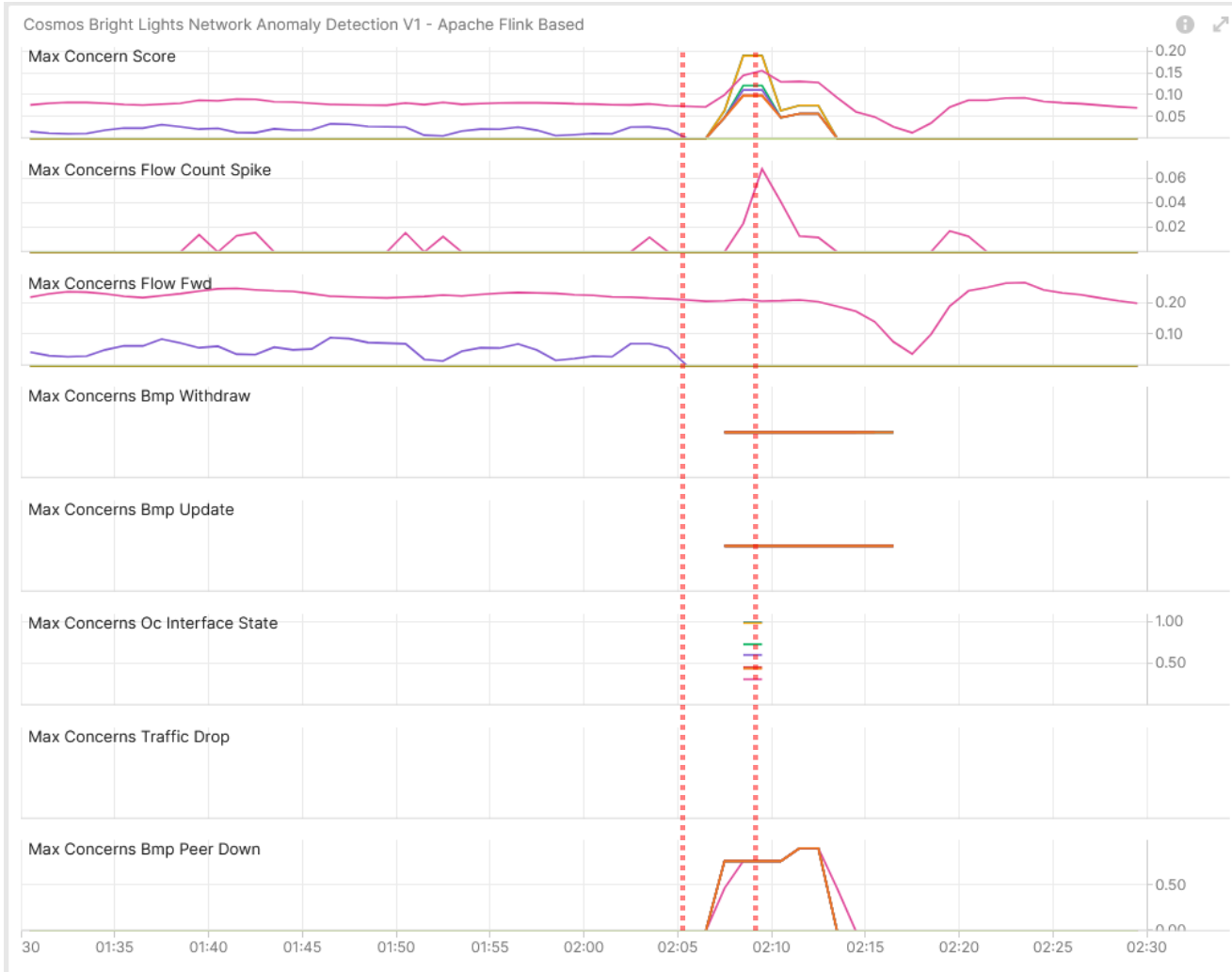
Shows **flow count spike** due to BGP topology change. Measured with **IPFIX** and Correlated with **BMP Local RIB**.

Shows **traffic shift** among Inter-AS Option A ASBR's. Measured with **YANG-Push openconfig-interface.yang**.

November 28th, SRv6 Resilience Analysis & Tests in Production

Use Case 1 – Network Anomaly Detection – Live

Concern Score: **0.19**
 Flow Count Spike: **0.07**
 Missing Traffic: **0.26**
 Traffic Drop: **0.00**
 BMP Peer/Interface Down: **0.91/0.99**
 BMP Update/Withdrawal: **0.00/0.00**



Cosmos Bright Lights Anomaly Detection – 8x L3 VPN's



BMP route-monitoring Update/Withdraw check did not recognize topology change.



BMP peer Down/Up check recognized BGP peering state change.



Interface Down/Up check recognized Interface state change.



Traffic Drop spike recognized did not apply.



Missing Traffic check recognized long term traffic loss on 64498:2949.



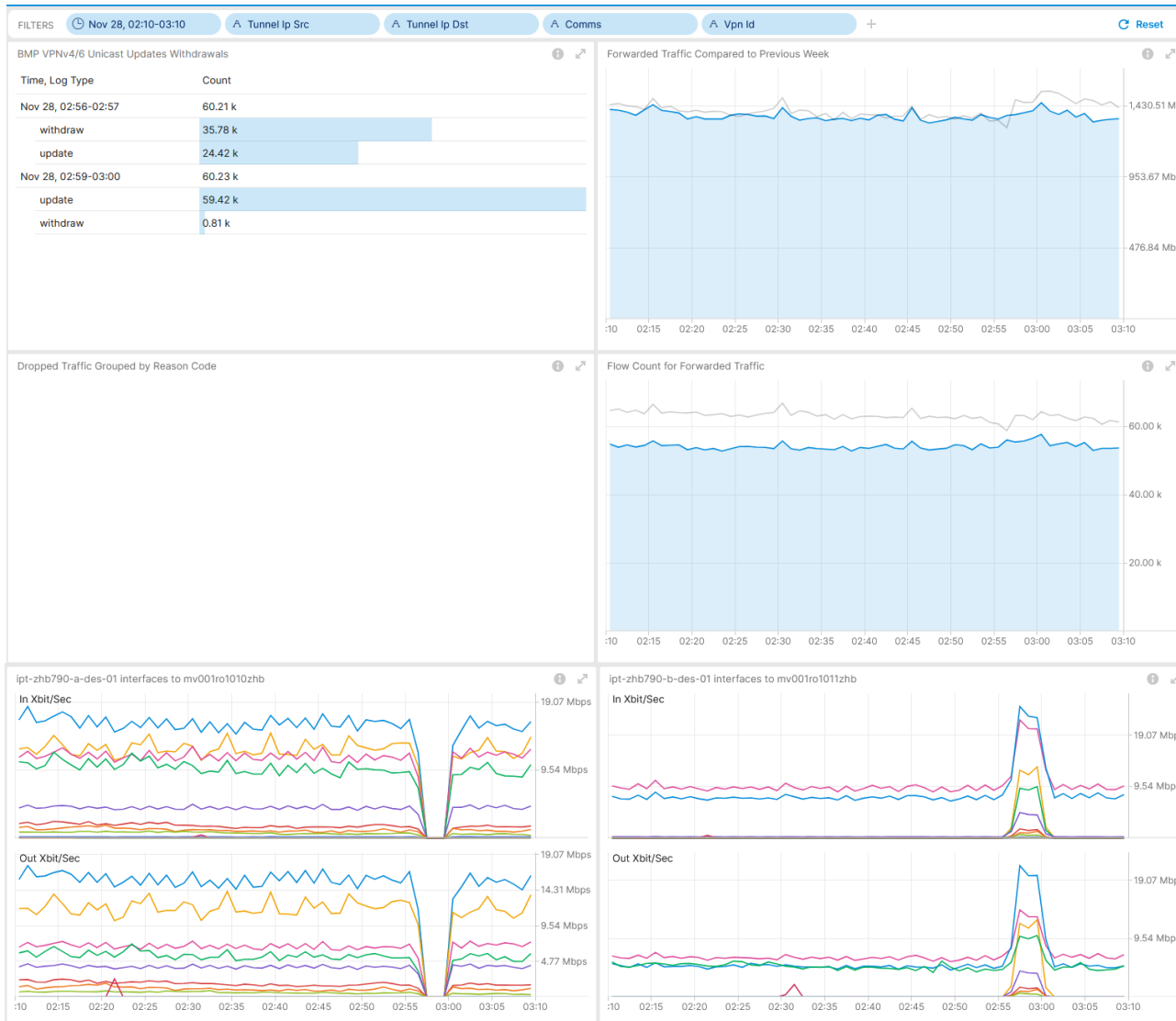
Increased or decreased Flow Count check did recognize flow spike decrease.



Overall: 4 out of 6 checks have detected the Interface and BGP topology change and flow count spike. Why BGP topology changes were not identified needs to be investigated.

November 28th, SRv6 Resilience Analysis & Tests in Production

Use Case 2 – Inter-AS Option A Interface State Change – **Real-Time** Maintenance Window Analysis



← Shows **BGP topology change** and no traffic volume change. Measured with IPFIX and Correlated with BMP Local RIB.

← Shows no flow count change. Measured with IPFIX and Correlated with BMP Local RIB.

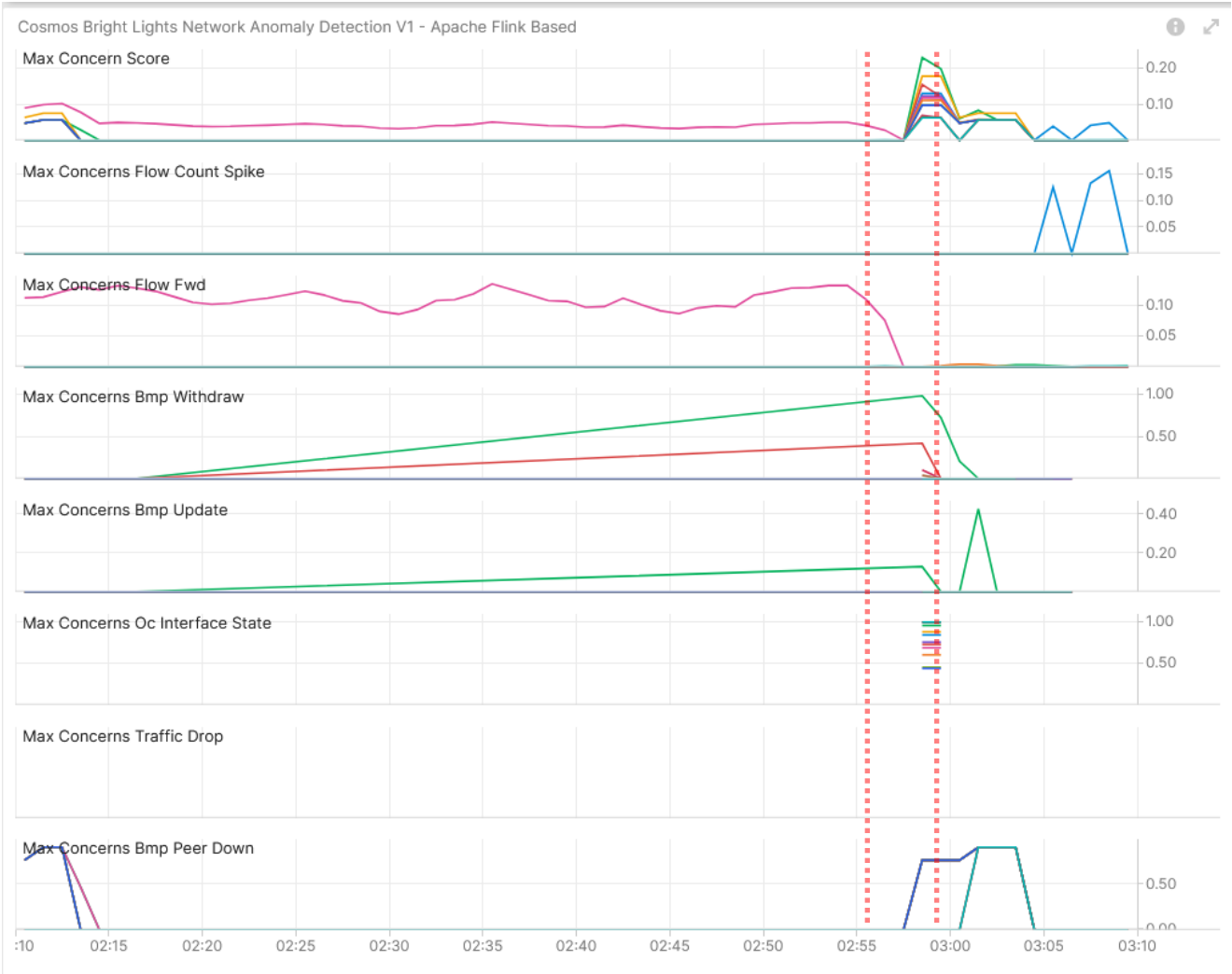
← Shows **traffic shift** among Inter-AS Option A ASBR's. Measured with YANG-Push openconfig-interface.yang.

Operational Network Telemetry forwarding plane, YANG-Push, IPFIX, BMP and BGP measured control plane metrics.








November 28th, SRv6 Resilience Analysis & Tests in Production

Use Case 2 – Network Anomaly Detection – Live

Concern Score: 0.23
 Flow Count Spike: **0.16**
 Missing Traffic: **0.00**
 Traffic Drop: **0.00**
 BMP Peer/Interface Down: **0.91/1.00**
 BMP Update/Withdrawal: **0.43/0.98**



Cosmos Bright Lights Anomaly Detection – 12x L3 VPN's

-  **BMP route-monitoring Update/Withdraw check recognized topology change.**
-  **BMP peer Down/Up check recognized BGP peering state change.**
-  **Interface Down/Up check recognized Interface state change.**
-  Traffic Drop spike recognized did not apply.
-  **Missing Traffic check did not apply.**
-  **Increased or decreased Flow Count check did recognize flow spike increase.**
-  **Overall: 5 out of 6 checks have detected the interface and BGP topology change and flow count spike. Meets perfectly our expectations.**

November 28th, SRv6 Resilience Analysis & Tests in Production

Use Case 3 – SRv6 Provider Interface State Change – Real-Time Maintenance Window Analysis



← Shows **BGP topology change and brief missing traffic volume.** Measured with IPFIX and Correlated with BMP Local RIB.

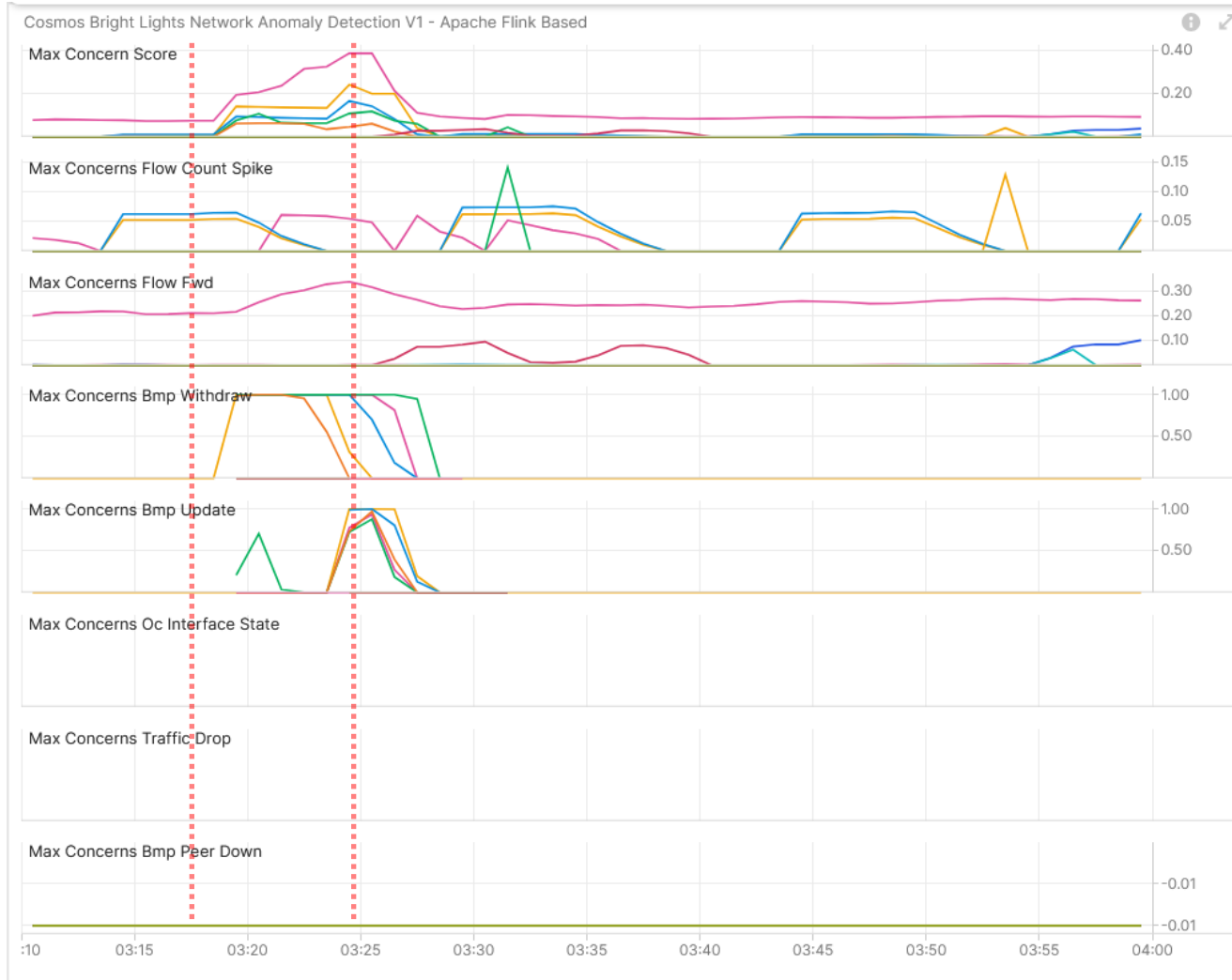
← Shows **brief flow count change.** Measured with IPFIX and Correlated with BMP Local RIB.

← Shows **traffic shift among Inter-AS Option A ASBR's.** Measured with YANG-Push openconfig-interface.yang.

November 28th, SRv6 Resilience Analysis & Tests in Production

Use Case 3 – Network Anomaly Detection – Live

Concern Score: 0.39
 Flow Count Spike: **0.14**
 Missing Traffic: **0.34**
 Traffic Drop: **0.00**
 BMP Peer/Interface Down: **0.00/0.00**
 BMP Update/Withdrawal: **1.00/1.00**



Cosmos Bright Lights Anomaly Detection – 16x L3 VPN's



BMP route-monitoring Update/Withdraw check recognized topology change.



BMP peer Down/Up check did not apply.



Interface Down/Up did not apply.



Traffic Drop spike recognized did not apply.



Missing Traffic check did not recognize brief traffic loss.



Increased or decreased Flow Count check did not recognize decreased and increased flow count spike.



Overall: 1 out of 6 checks have detected the BGP topology change. Missing traffic and Flow Count changes are hard to recognize when many changes occur in short period of time. Nevertheless, lets investigate wherever we have a chance to improve.

November 28th, SRv6 Resilience Analysis & Tests in Production

Use Case 4 – BGP Process Restart – **Real-Time** Maintenance Window Analysis



← Shows **BGP topology change**. Measured with IPFIX and Correlated with BMP Local RIB.

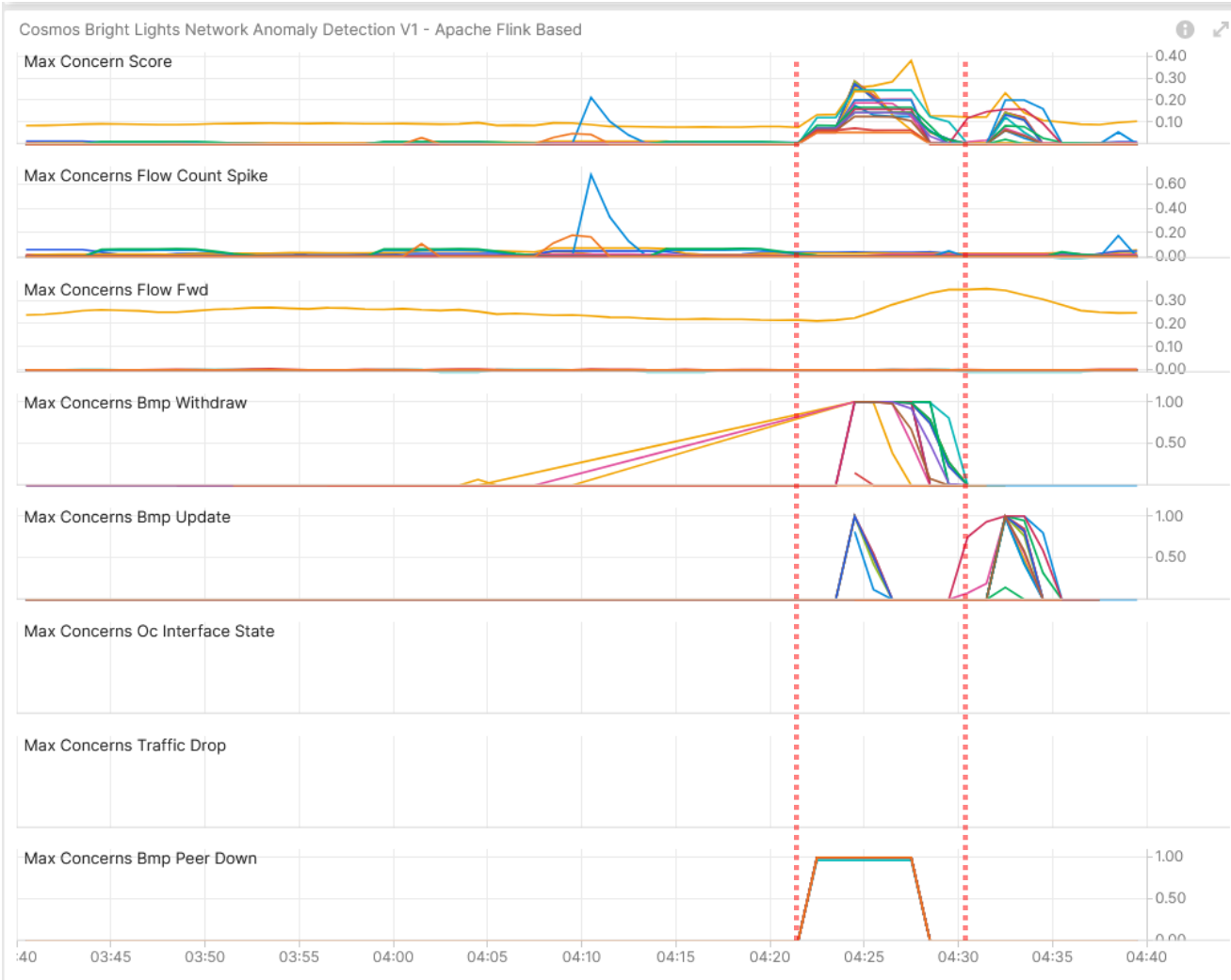
← Shows **no change in drops or flow count**. Measured with IPFIX and Correlated with BMP Local RIB.

← Shows **traffic shift among Inter-AS Option A ASBR's**. Measured with YANG-Push openconfig-interface.yang.








November 28th, SRv6 Resilience Analysis & Tests in Production

Use Case 4 – Network Anomaly Detection – Live

Concern Score: 0.38
 Flow Count Spike: **0.04**
 Missing Traffic: **0.35**
 Traffic Drop: **0.00**
 BMP Peer/Interface Down: **1.00/0.00**
 BMP Update/Withdrawal: **1.00/1.00**



Cosmos Bright Lights Anomaly Detection – 19x L3 VPN's

-  **BMP route-monitoring Update/Withdraw check recognized topology change.**
-  **BMP peer Down/Up check recognize peering state changes.**
-  Interface Down/Up did not apply.
-  Traffic Drop spike recognized did not apply.
-  **Missing Traffic check recognized long term traffic loss on 64498:2949.**
-  Increased or decreased Flow Count check did not apply.
-  **Overall: 2 out of 6 checks have detected the BGP topology and peering state change. Meets perfectly our expectations.**

November 28th, SRv6 Resilience Analysis & Tests in Production

Use Case 5– IS-IS Process Restart – **Real-Time** Maintenance Window Analysis



Shows **BGP topology change**. Measured with **IPFIX** and Correlated with **BMP Local RIB**.



Shows **drop adjacency**. Measured with **IPFIX** and Correlated with **BMP Local RIB**.



Shows **brief traffic shift** among Inter-AS Option A ASBR's. Measured with **YANG-Push openconfig-interface.yang**.

November 28th, SRv6 Resilience Analysis & Tests in Production


Use Case 5 – Network Anomaly Detection – Live

Concern Score: 0.53
 Flow Count Spike: **0.25**
 Missing Traffic: **0.27**
 Traffic Drop: **1.00**
 BMP Peer/Interface Down: **0.00/0.00**
 BMP Update/Withdrawal: **1.00/1.00**




Cosmos Bright Lights Anomaly Detection – 19x L3 VPN's


 **BMP route-monitoring Update/Withdraw check recognized topology change.**


 BMP peer Down/Up check did not apply.

 Interface Down/Up did not apply.

 **Traffic Drop spike recognized topology change.**

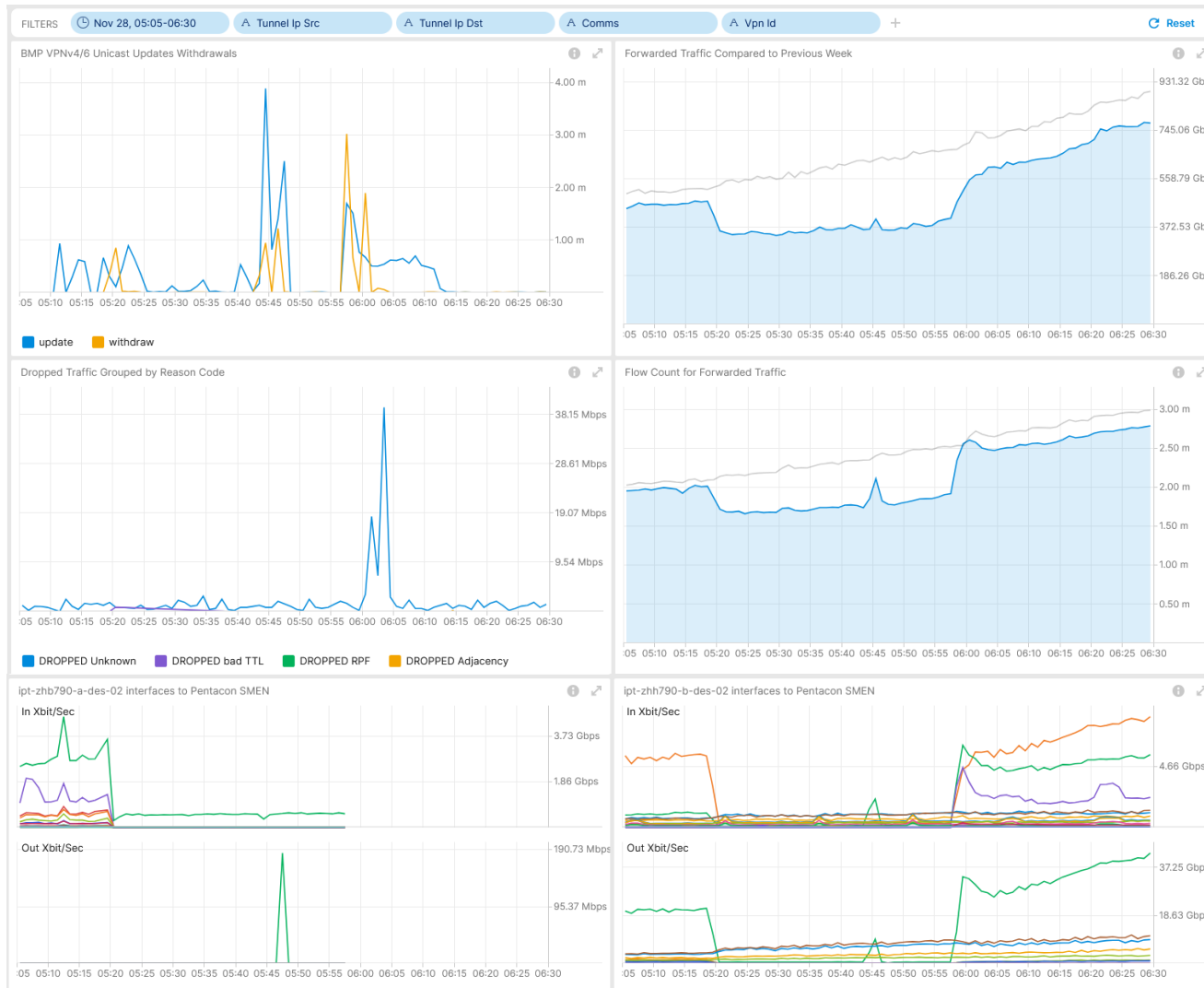
 **Missing Traffic check recognized long term traffic loss on 64498:2949.**

 Increased or decreased Flow Count check did not apply.

 **Overall: 2 out of 6 checks have detected the BGP topology change, and traffic drop spike. Meets perfectly our expectations.**

November 28th, SRv6 Resilience Analysis & Tests in Production

Use Case 6– RSP Failover – Real-Time Maintenance Window Analysis



Shows **BGP topology change and missing traffic during blackholing**. Measured with IPFIX and Correlated with BMP Local RIB.



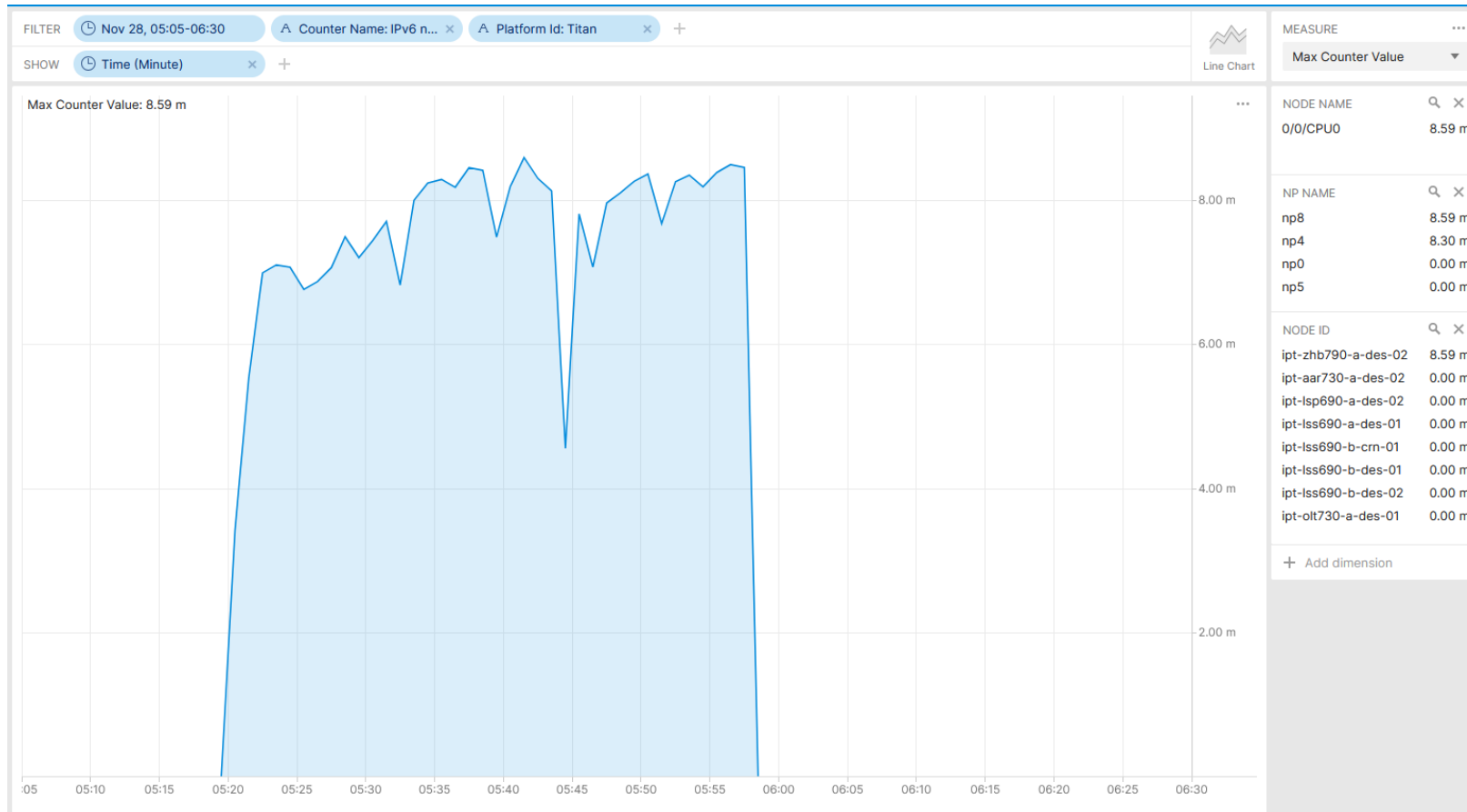
Shows **drop unknown at recovery and reduced flow count during blackholing**. Measured with IPFIX and Correlated with BMP Local RIB.



Shows **traffic shift among Inter-AS Option A ASBR's**. Measured with YANG-Push openconfig-interface.yang.

November 28th, SRv6 Resilience Analysis & Tests in Production

IPv6 next-hop index invalid transmit adjacency drops - **Real-Time** Maintenance Window Analysis

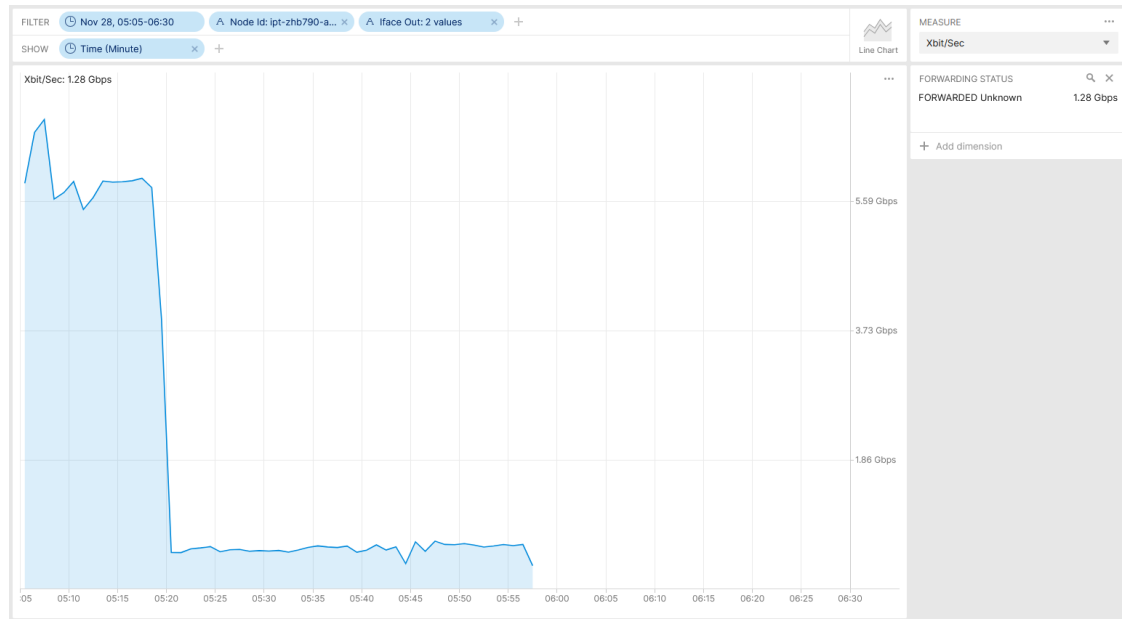
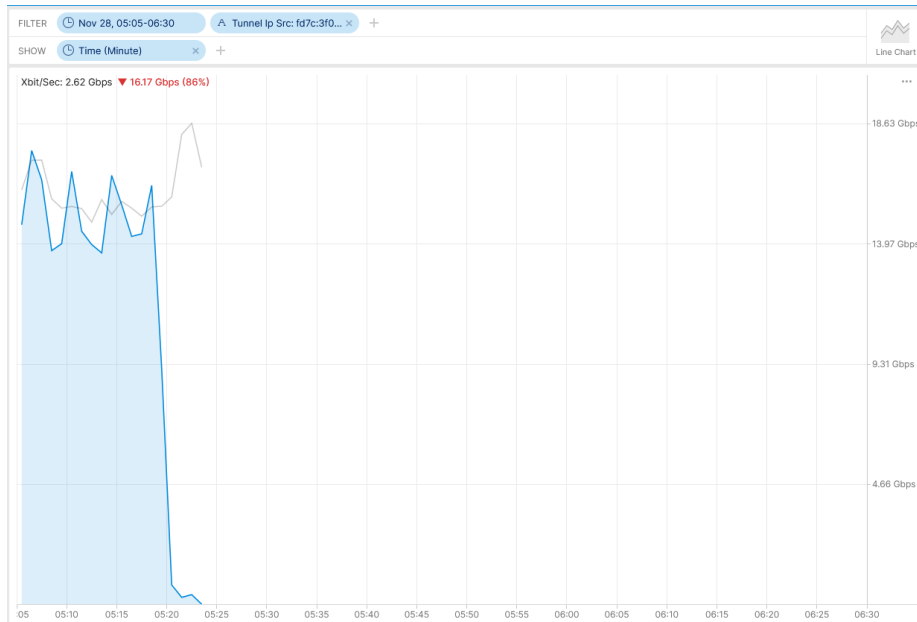


Shows **egress NPU drops** on NPU 4 and 8 on line card 0/0/CPU0 at ipt-zhb790-a-des-02. Measured with YANG-Push.

Operational Network Telemetry YANG-Push collected NPU drop counter (IPv6 next-hop index invalid transmit adjacency) metrics.

November 28th, SRv6 Resilience Analysis & Tests in Production

IPFIX does not recognize at ingress the egress drop - **Real-Time** Maintenance Window Analysis



Shows that ingress captured traffic is **measured forwarded mistakenly**, however then dropped at egress on **ipt-zhb790-a-des-02**. **Measured with IPFIX in different parts of the SRv6 domain.**

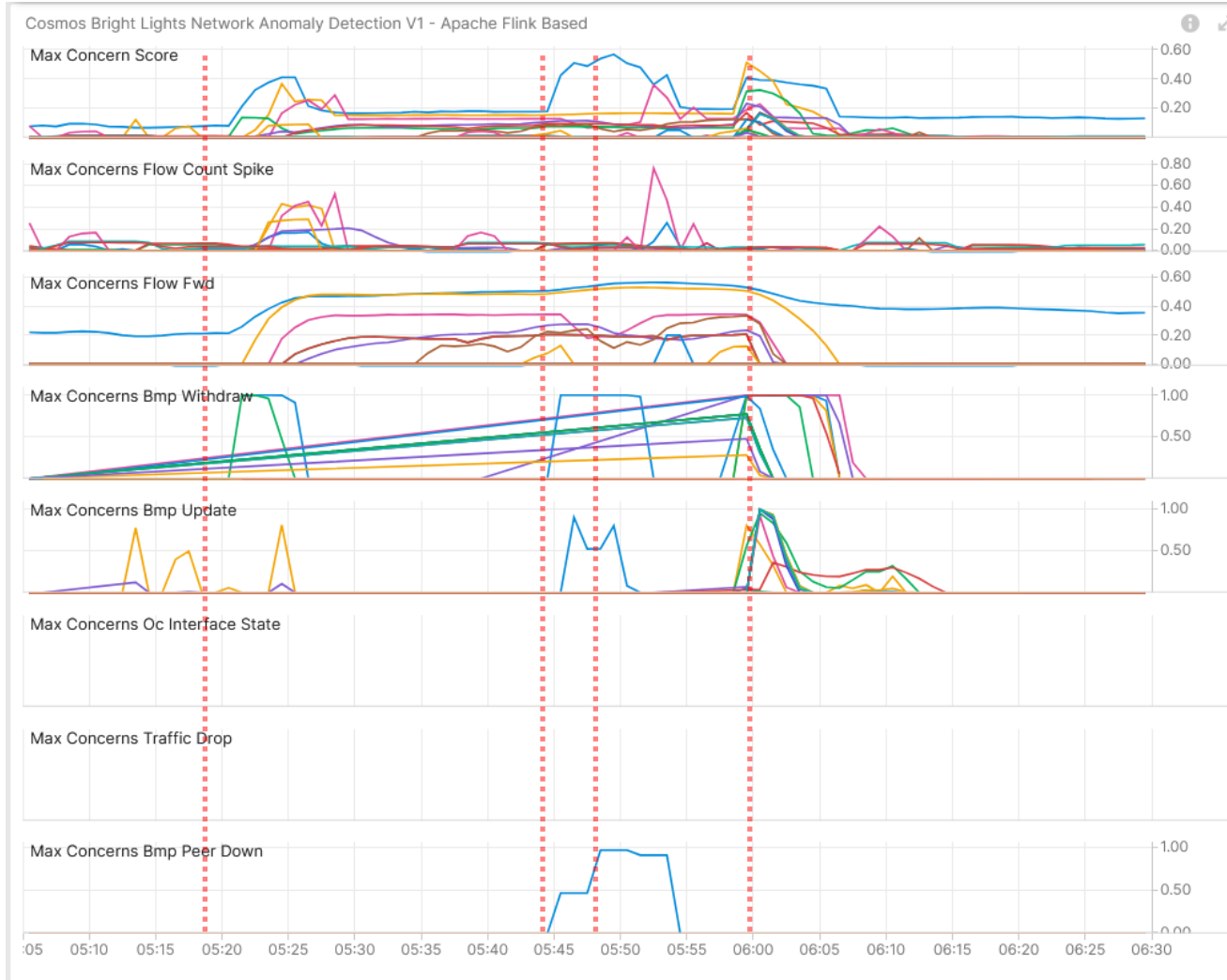
Operational Network Telemetry IPFIX collected metrics showing traffic **originated by IPv6 Tunnel source fd7c:3f00:f06::1 (ipt-zhb790-a-des-02)**.

Operational Network Telemetry IPFIX collected metrics showing traffic on **Bundle-Ether2000 and Bundle-Ether2100 egress (SRv6 P) at ipt-zhb790-a-des-02 captured ingress**.








November 28th, SRv6 Resilience Analysis & Tests in Production

Use Case 6 – Network Anomaly Detection – Live

Concern Score: 0.57
 Flow Count Spike: **0.76**
 Missing Traffic: **0.57**
 Traffic Drop: **0.00**
 BMP Peer/Interface Down: **0.00/0.96**
 BMP Update/Withdrawal: **1.00/1.00**



Cosmos Bright Lights Anomaly Detection – 19x L3 VPN'

-  **BMP route-monitoring Update/Withdraw check recognized topology change.**
-  **BMP peer Down/Up check recognized peering state changes.**
-  Interface Down/Up did not apply.
-  Traffic Drop spike did not apply since IPFIX did not recognize egress drop.
-  **Missing Traffic check recognized blackholing.**
-  **Increased or decreased Flow Count check recognize drop spike due to topology change.**
-  **Overall: 4 out of 6 checks have detected the BGP topology change, missing traffic and traffic drop spike. Meets perfectly our expectations.**

What to do next?

- > Evaluate why in use case 1 BGP topology changes were not recognized.
-> Ongoing.
- > Evaluate if in use case 3 Missing traffic and flow count changes could be detected.
-> Ongoing.
- > Clarify wherever egress IPFIX could have identified drops.
-> Done.
- > Persist operational data in TSDB for training purposes.
-> Done.



What went well?



IPFIX, BMP and YANG-Push delivered the almost perfect operational view on the impacted network.



Cosmos Bright Lights Network Anomaly Detection was battelled in a series of tests and showed that is more than just ready for production. **It excels in most of the areas.**



We are real-time. BGP topology changes within 3 seconds. Interface traffic within 60 seconds. IPFIX flow aggregation within 90 seconds. Network Anomaly Detection within 180 seconds.



What could be improved?



Detect egress drops on data plane serialization in IPFIX.



Include NPU drop verification in resilience analysis and add semantics in Cisco-IOS-XR-asr9k-np-oper.yang describing drop counter meaning.

Add "Cisco-IOS-XR-wdsysmon-fd-oper:system-monitoring/cpu-utilization" xpath in YANG-Push configuration.



Restart of IS-IS process would have no impact if Network Telemetry transport sessions would have been established outband.



Cisco TAC having access to operative Network Telemetry and network node software process, management plane, tracing data.