

Observing trends in Internet routing security

Iliana Xyengkou*, Cecilia Testart, Alberto Dainotti
{ixyengkou3, ctestart, dainotti}@gatech.edu
November 01, 2024

**Scholar of the Onassis Foundation*



Key question

What do we know about routing incidents?

Key question

What do we know about
routing incidents?

Key question

What do we know about
routing incidents?



**Abuse
Misconfiguration**

Key question

What do we know about
routing incidents?

**Abuse
Misconfiguration**

**Hijacking
Fat-finger
Route Leaks**

Key question

What do we know about
routing incidents?

**Abuse
Misconfiguration**

**Hijacking
Fat-finger
Route Leaks**

**Disruption
Impersonation
Eavesdropping**

GRIP – <https://bgp.live> (grip.inetintel.cc.gatech.edu)



- Been around since ~2018 (CAIDA); running @ GATech since 2021
- Public dashboard + API; Open source
- Main BGP incidents datasource to the MANRS observatory
- Annotation and inference methods constantly improving
- Current status: We reprocessed the last 5 years to uncover trends

Global Routing Intelligence Platform

Select an event type: All MOAS Sub-MOAS New Edge Defcon
Select an event suspicion level: All Suspicious Grey Benign
Select time period (UTC now: Jun 22, 2023 3:16 AM): Jun 20, 2023 9:41 PM - Jun 21, 2023 9:41 PM
Search for events by prefix/ASN/tags: Search by prefix/ASN/tags Search

Events List

Potential Victims	Potential Attackers	Largest (Sub)Prefix	# Prefix Events	Start Time	Duration
AS39369 Avallo Networks AB	AS29468 InfraCom Mana...ces AB	192.176.123.0/24	1	2023-06-21 20:20	10 min
AS16150 AVALLO NETWORKS AB	AS29468 InfraCom Mana...ces AB	194.71.157.0/24	2	2023-06-21 20:10	25 min
AS203100 Iman Samaneh ...hr LLC	AS41689 Asiotech Data...ompany	185.141.244.0/24	1	2023-06-21 19:10	5 min
AS269343 CRISTIANO FRA...ROS ME	AS53013 W I X NET DO...A - ME	45.184.204.0/22	1	2023-06-21 18:50	10 min
AS269577 INFOVIRTUAL S...TDA ME	AS28598 MOB SERVICOS ...S S.A.	45.189.46.0/24	1	2023-06-21 18:25	25 min
AS133199 SonderCloud Limited	AS18013 ASLINE LIMITED AS133861 HUPO LIMITED	45.207.56.0/24	1	2023-06-21 16:15	5 min
AS141893 PT Kawanua In...onesia	AS139982 PT Buana Visu...Sentra	103.162.114.0/23	1	2023-06-21 16:15	5 min
AS52698 OPENTEL Comér...s Ltda	AS5 WFA Group LLC	177.73.68.0/24	4	2023-06-21 15:35	ongoing
AS3356 Level 3 Parent, LLC	AS27341 Gannet Flemin..., Inc.	216.174.25.0/24	1	2023-06-21 15:35	5 min
AS52698 OPENTEL Comér...s Ltda	AS4 University of...ornia AS5 WFA Group LLC	177.73.68.0/24	4	2023-06-21 15:30	5 min

Rows per page: 10 1-10 of 21 |< < > >|

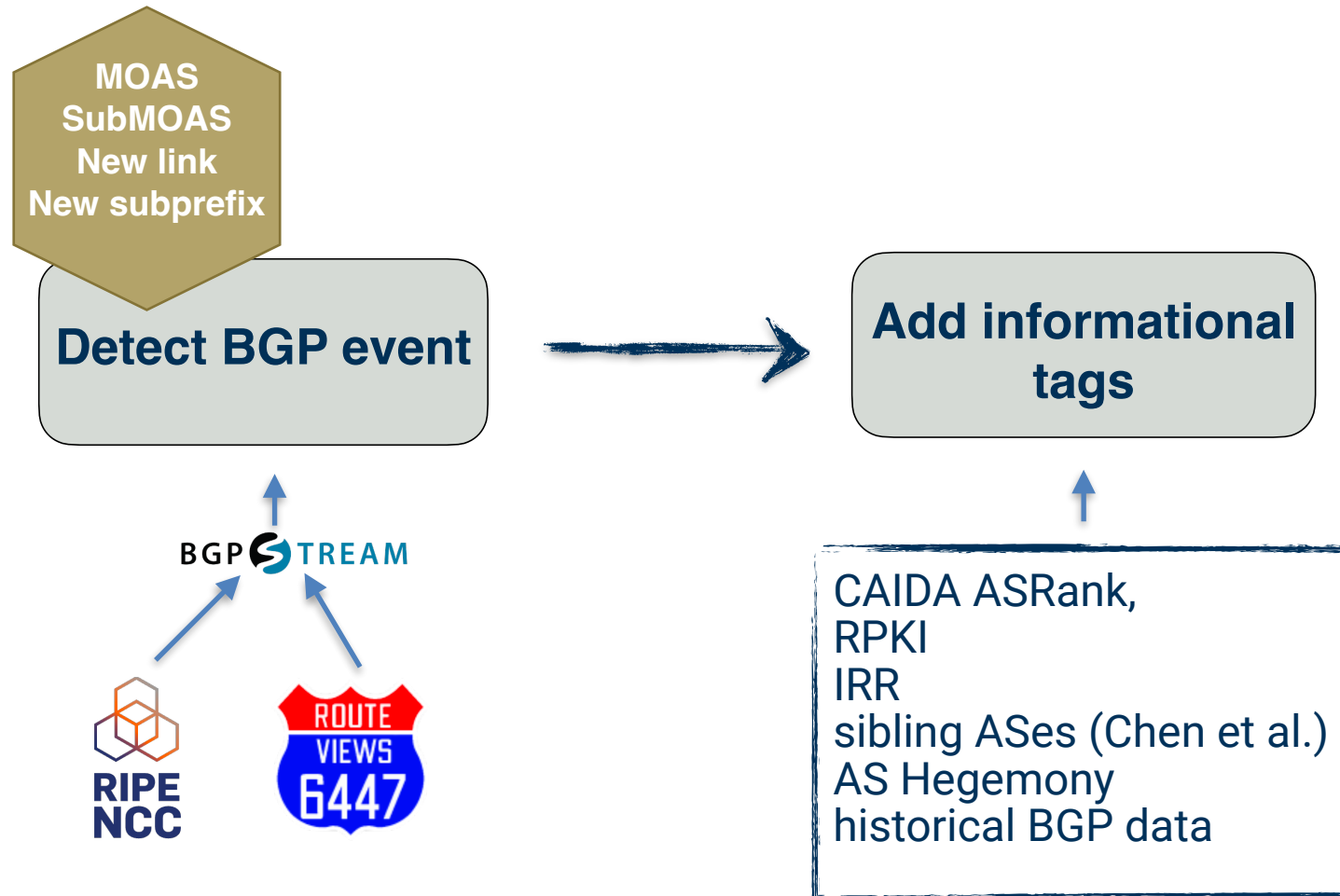
How does GRIP work?

- Target: *All* types of hijacking attacks and hijacking misconfigurations



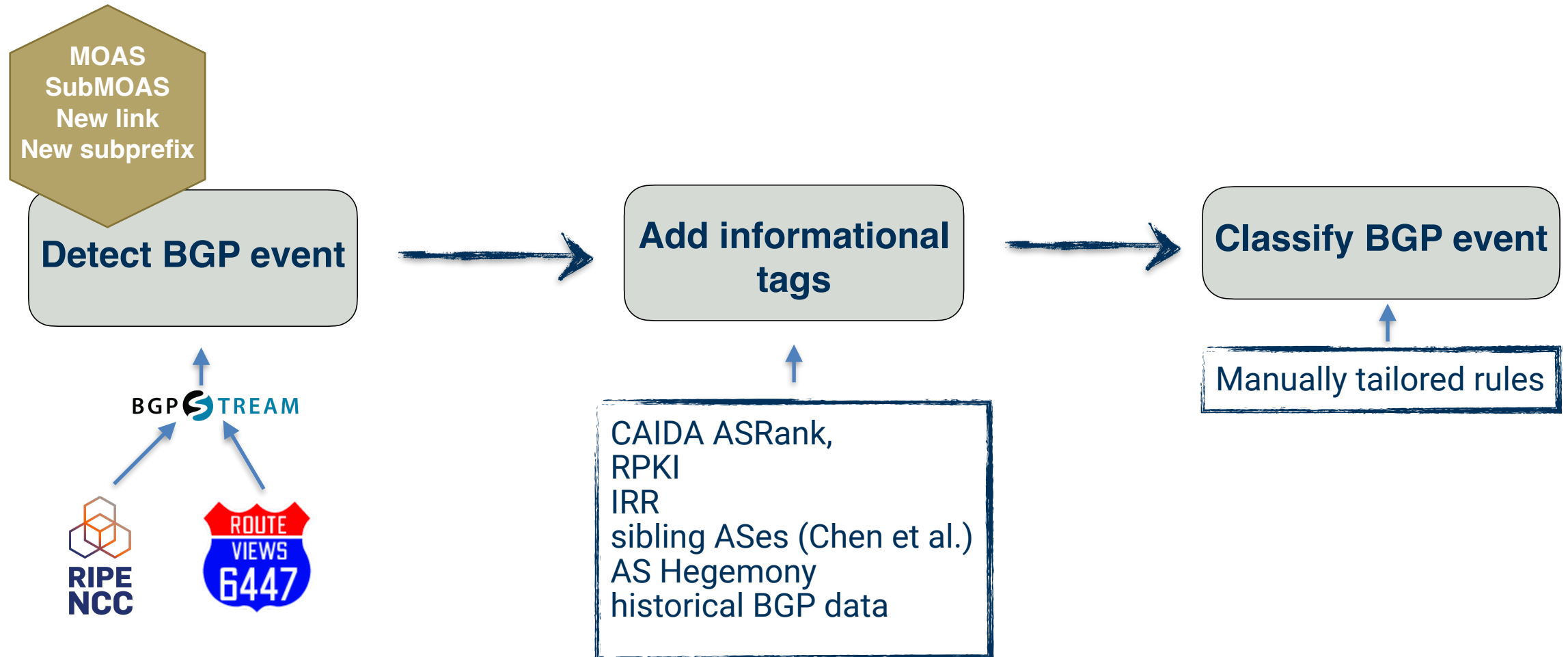
How does GRIP work?

- Target: *All* types of hijacking attacks and hijacking misconfigurations



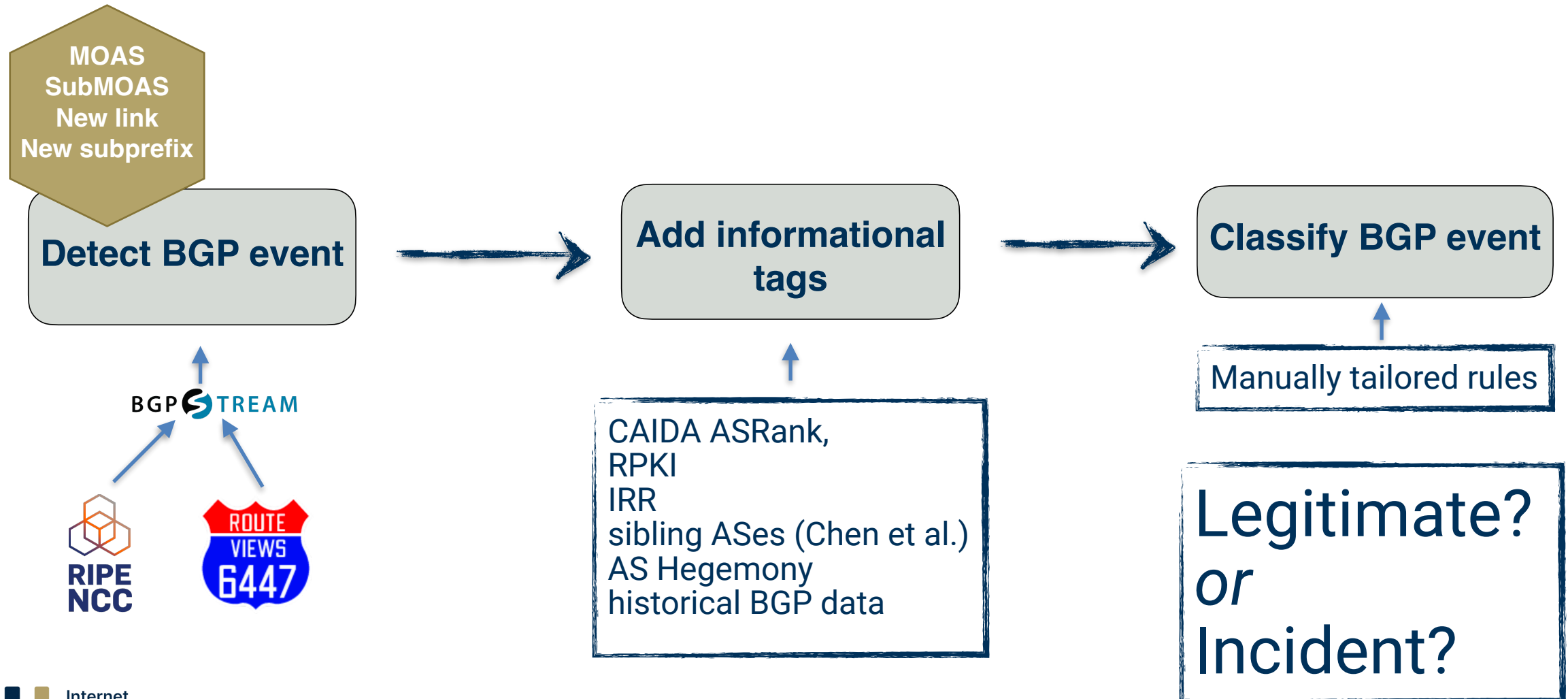
How does GRIP work?

- Target: *All* types of hijacking attacks and hijacking misconfigurations



How does GRIP work?

- Target: *All* types of hijacking attacks and hijacking misconfigurations



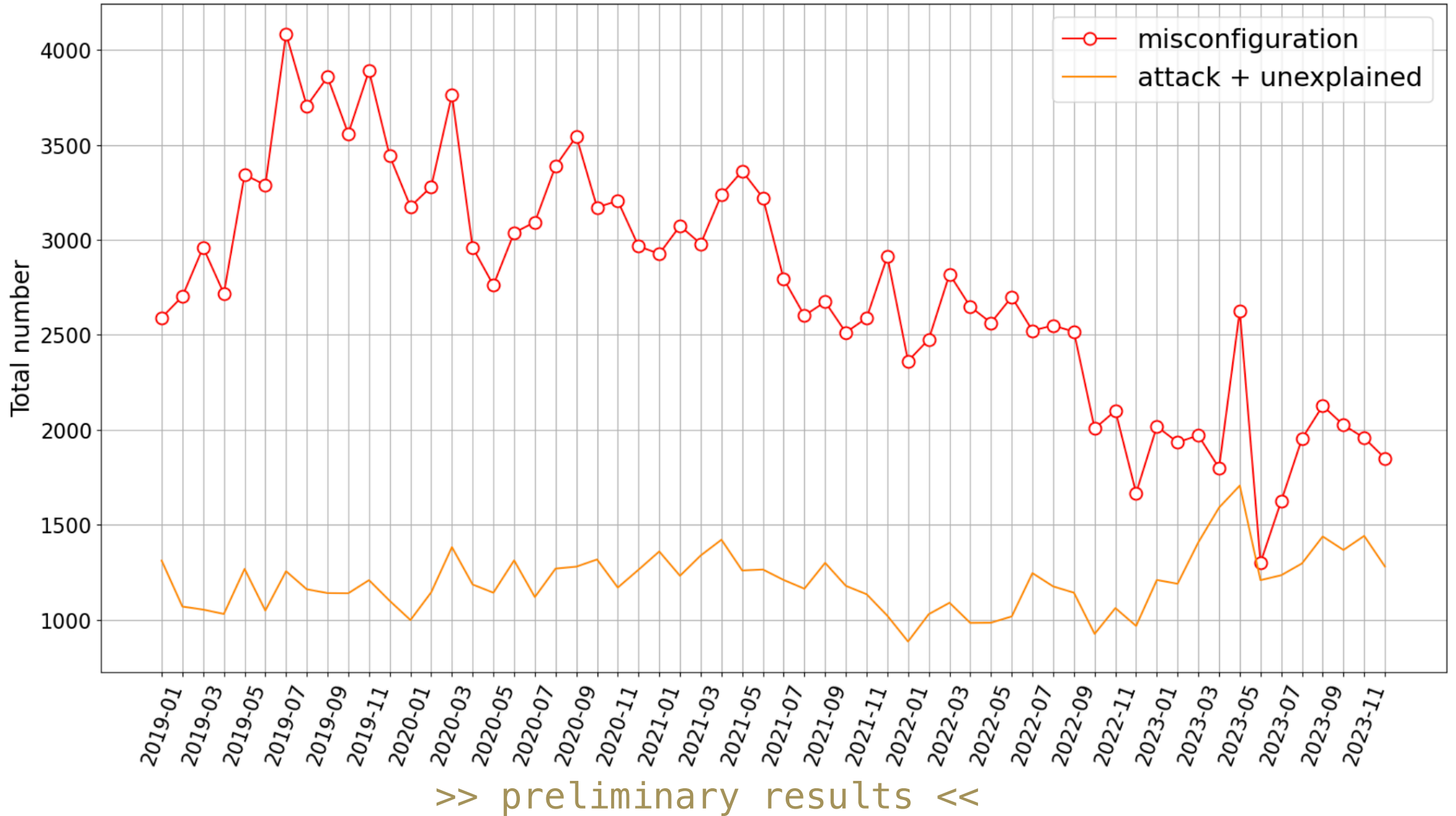
What have we observed so far?

Classification of events – where we are now



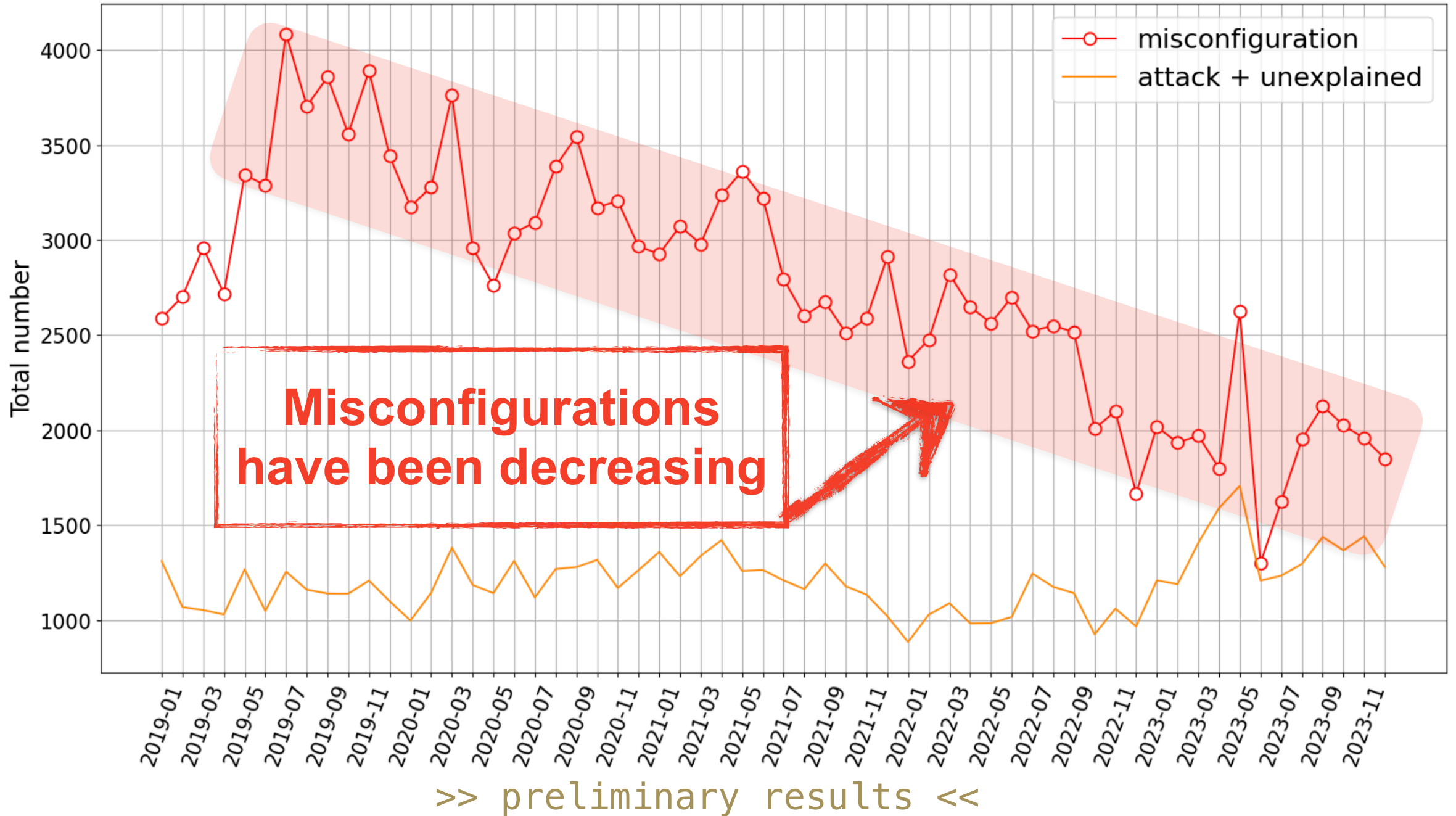
- We mark most of the events as legitimate [85%]
 - Most incidents show misconfiguration patterns [10%]
 - Fat finger of prefix/ASN
 - AS path prepending mistake (e.g., AS978, AS2 instead of AS978, AS978)
 - Related ASes but RPKI invalid ...
 - Many events w/ patterns of attacks [2%]
 - or misconfigs hard to diagnose → *E.g., RPKI invalid but owners failed to publish correct ROAs*
 - Unable to explain several events [2%]
- **Legitimate** 85%; ~280k/yr
 - **Incidents** 15%; ~50k/yr
 - **Misconfigs** 10%; 33k/yr
 - **Attacks** 2%; 7k/yr
 - **Unexplained** 2%; 7k/yr
 - **Abnormal** 1%; 3k/yr

Incidents

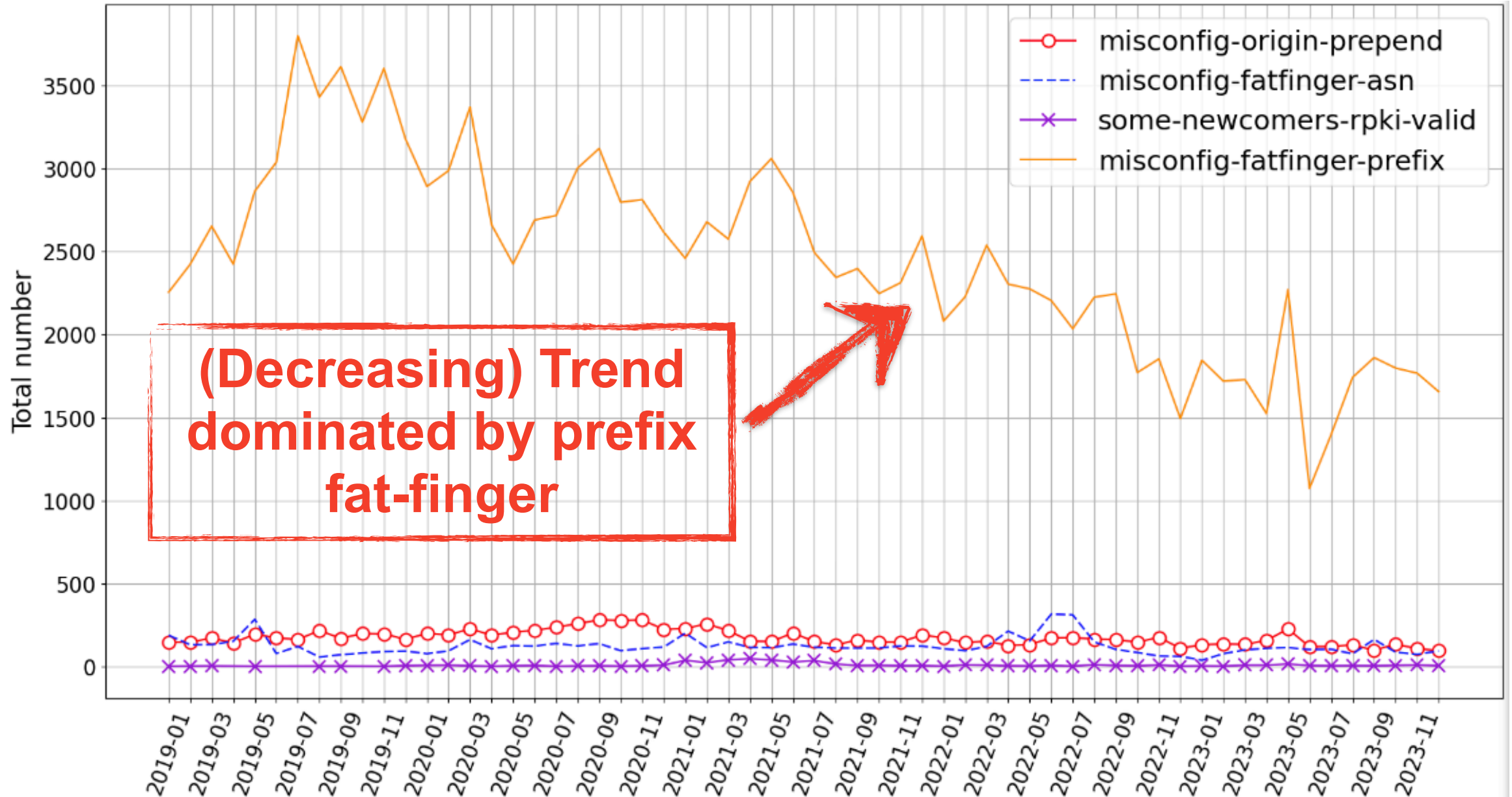


>> preliminary results <<

Incidents

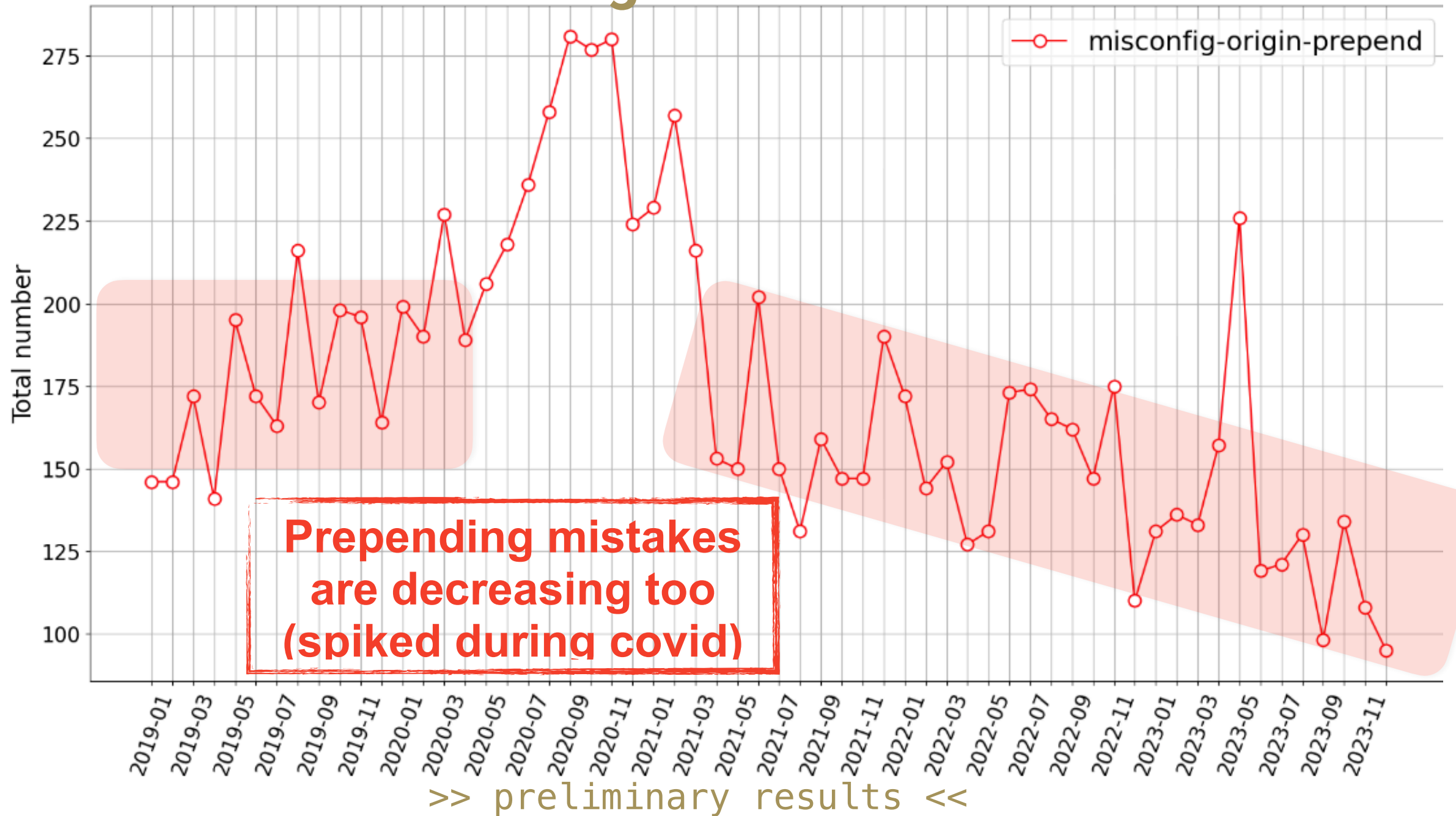


A closer look at misconfigurations

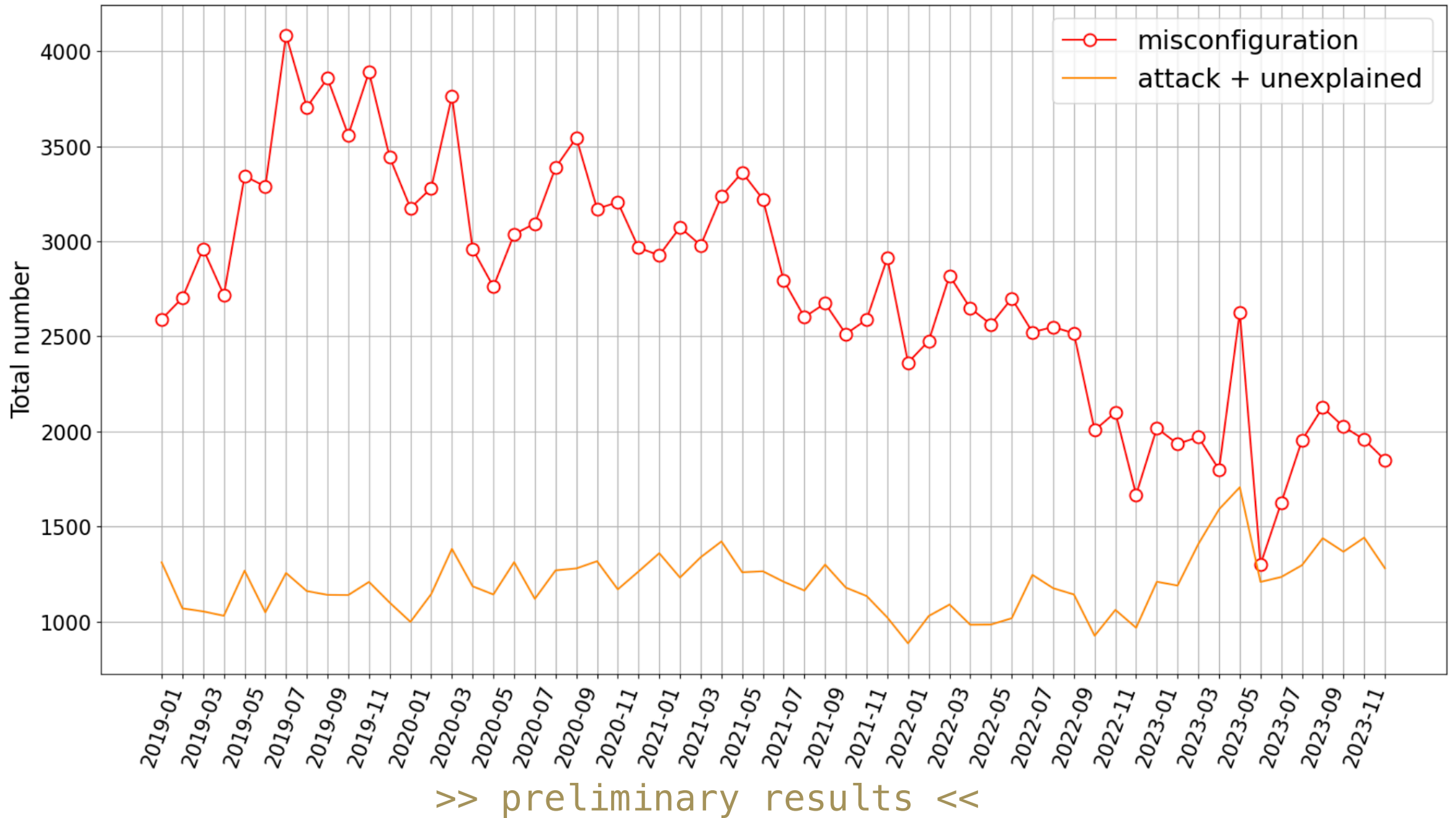


>> preliminary results <<

A closer look at misconfigurations

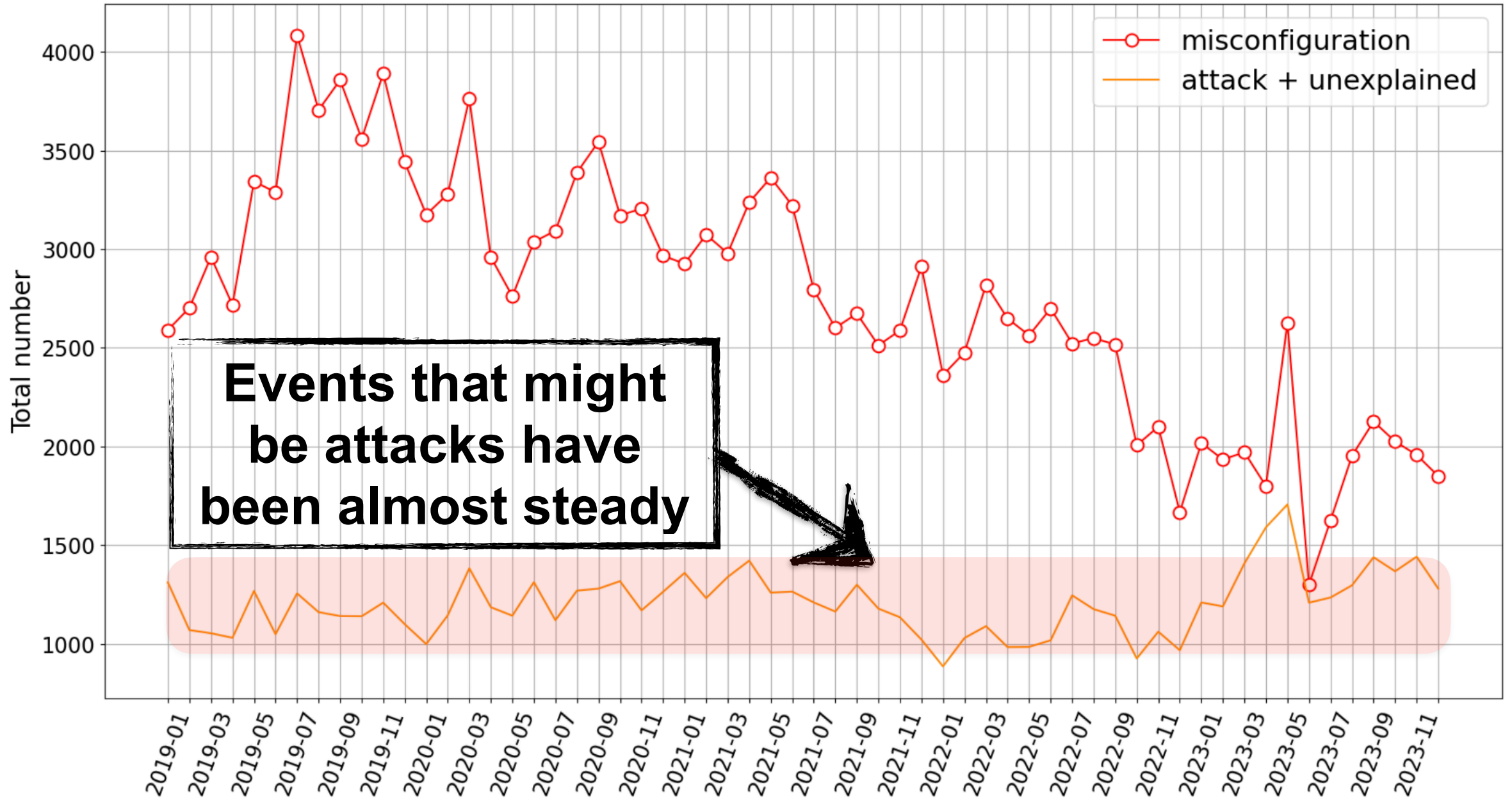


Incidents



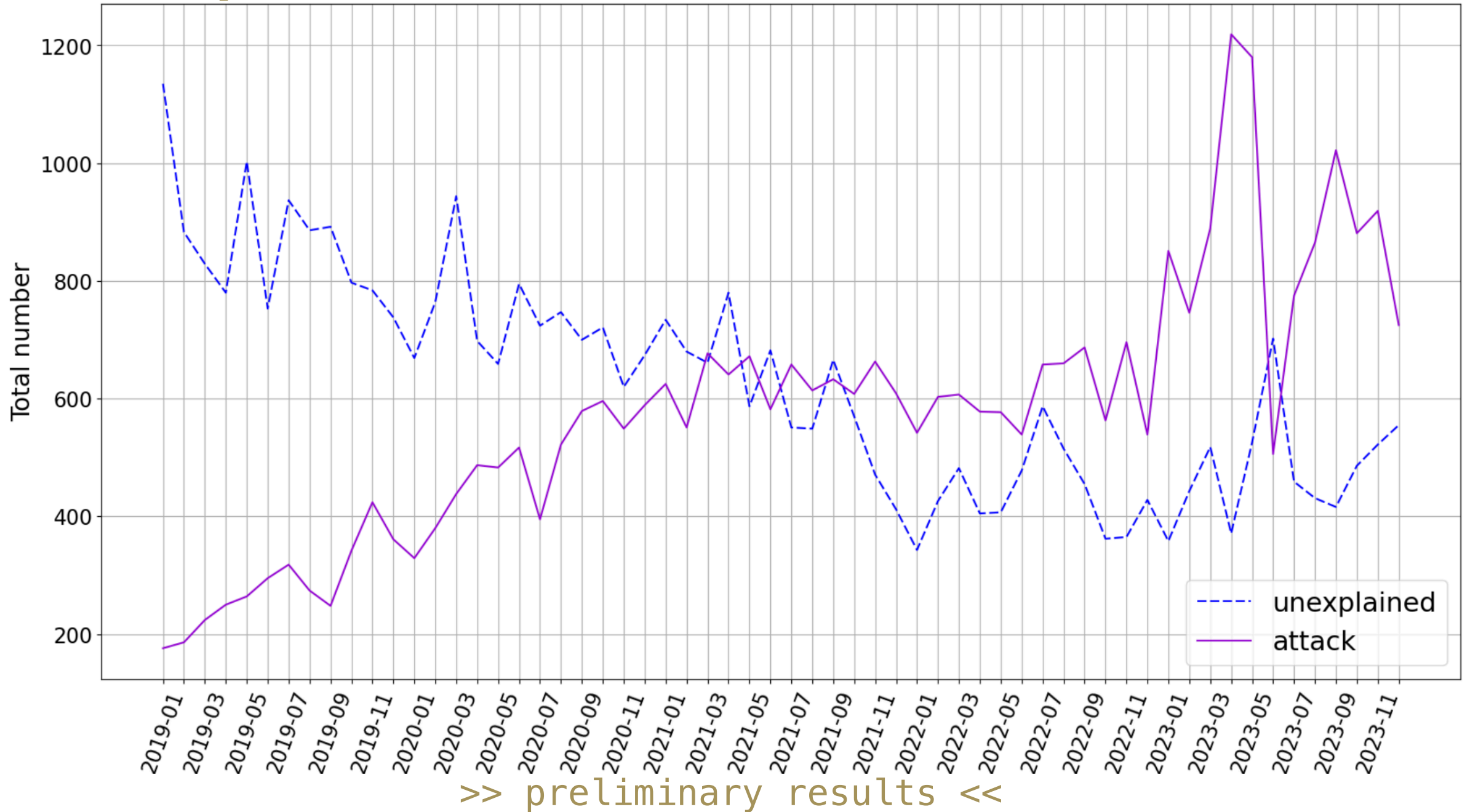
>> preliminary results <<

Incidents

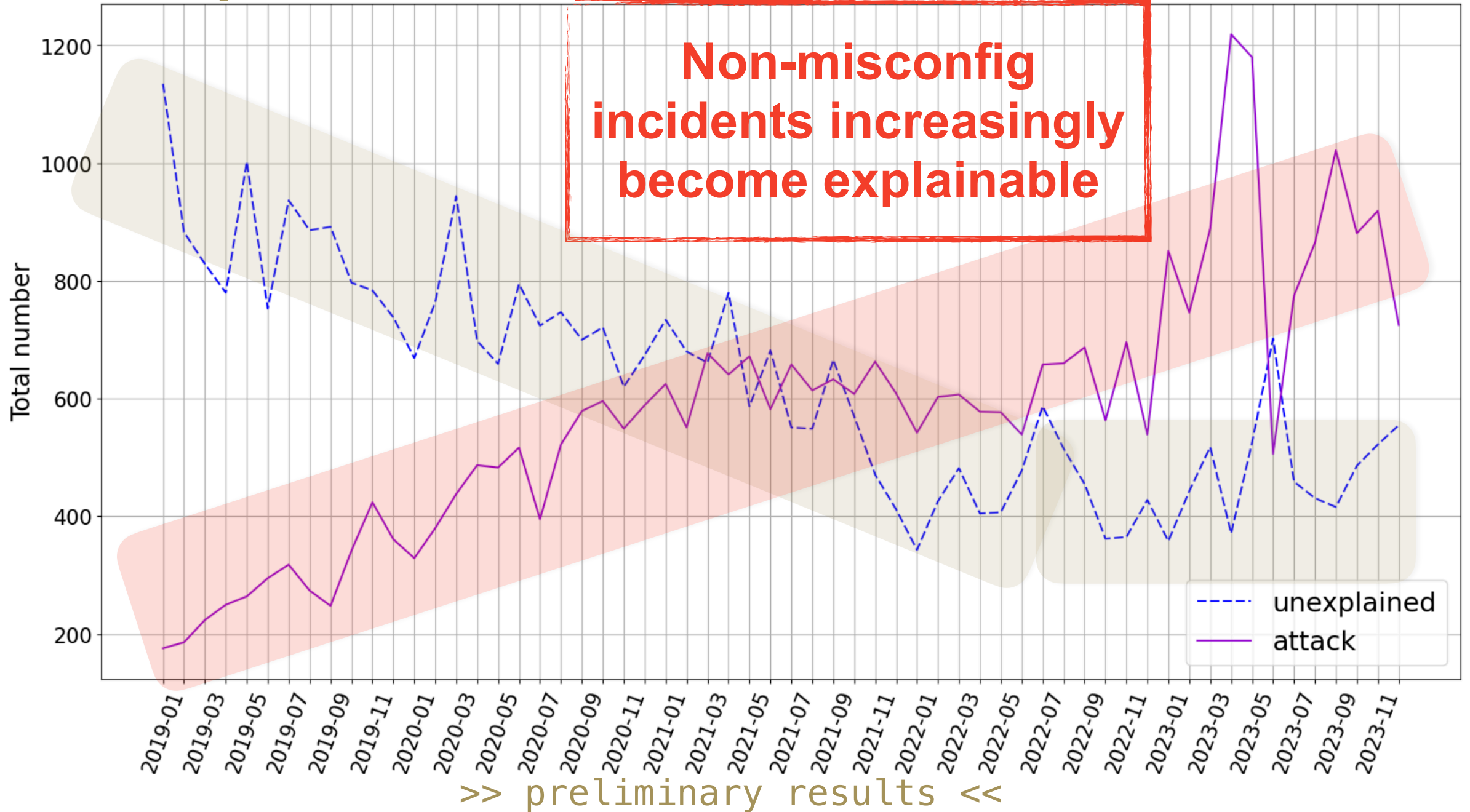


>> preliminary results <<

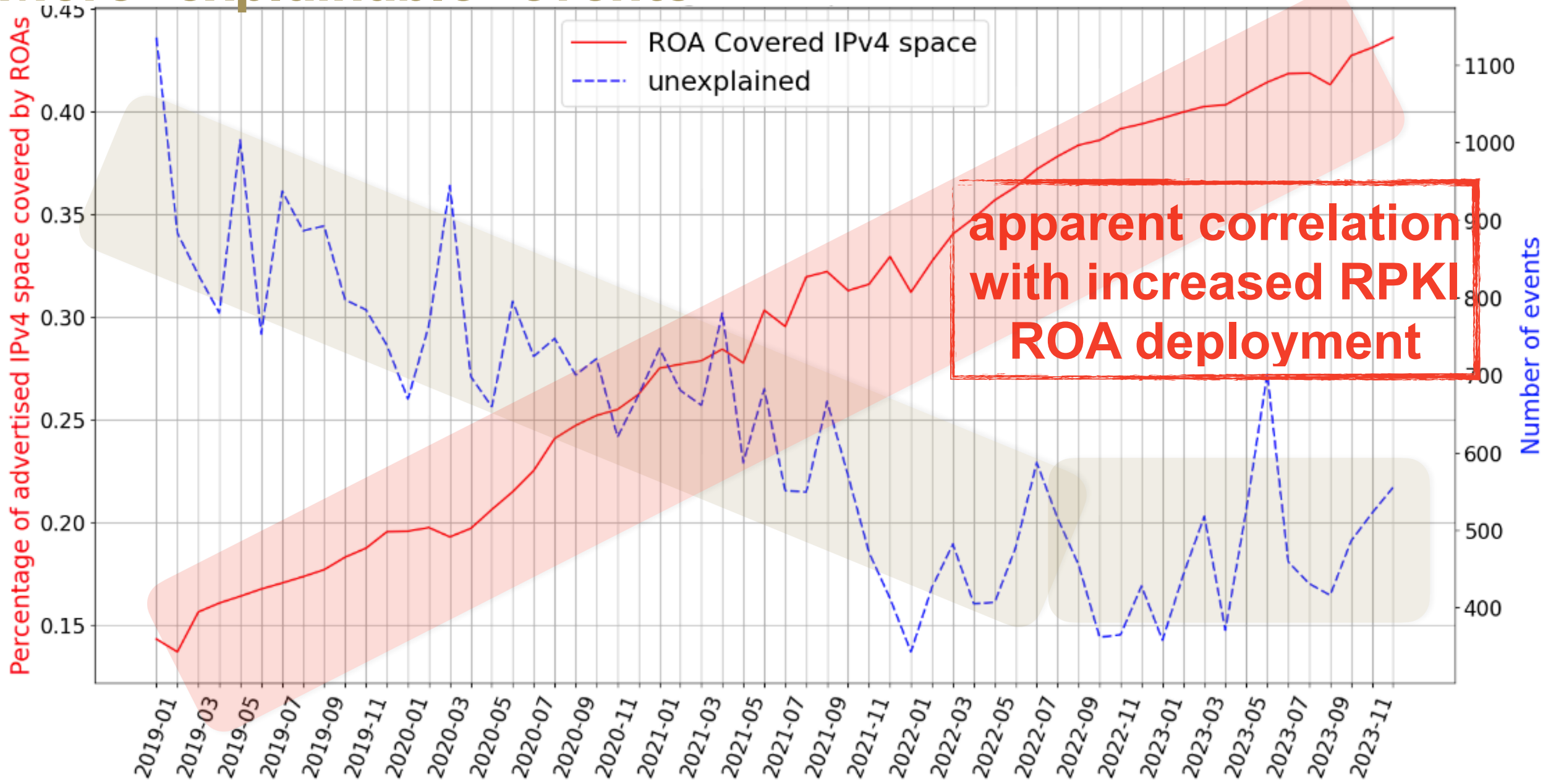
More “explainable” events



More “explainable” events



More “explainable” events



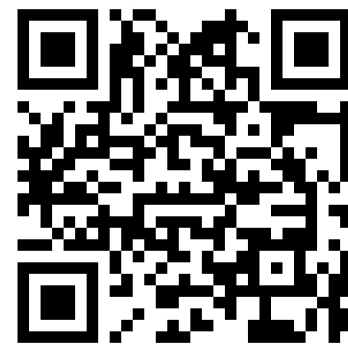
>> preliminary results <<

GRIP: How can we improve?



GRIP: How can we improve?

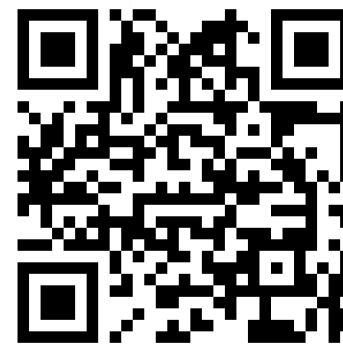
- Improve and add new inference logic
 - Validation / feedback from operators



bgp.live

GRIP: How can we improve?

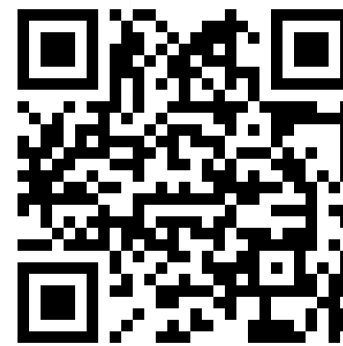
- Improve and add new inference logic
 - Validation / feedback from operators
- Improve reliability of operations
 - Infrastructure, developers, researchers



bgp.live

GRIP: How can we improve?

- Improve and add new inference logic
 - Validation / feedback from operators
- Improve reliability of operations
 - Infrastructure, developers, researchers

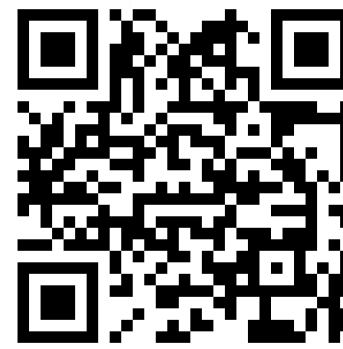


bgp.live

It takes a village (including you!) to build a reliable and usable tool that helps uncover what is happening in today's Internet and improve its security!

GRIP: How can we improve?

- Improve and add new inference logic
 - Validation / feedback from operators
- Improve reliability of operations
 - Infrastructure, developers, researchers



bgp.live

It takes a village (including you!) to build a reliable and usable tool that helps uncover what is happening in today's Internet and improve its security!

Thank you!