Observing trends in Internet routing security

Iliana Xygkou*, Cecilia Testart, Alberto Dainotti
{ixygkou3, ctestart, dainotti}@gatech.edu
November 01, 2024

*Scholar of the Onassis Foundation

Internet Intelligence Lab

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

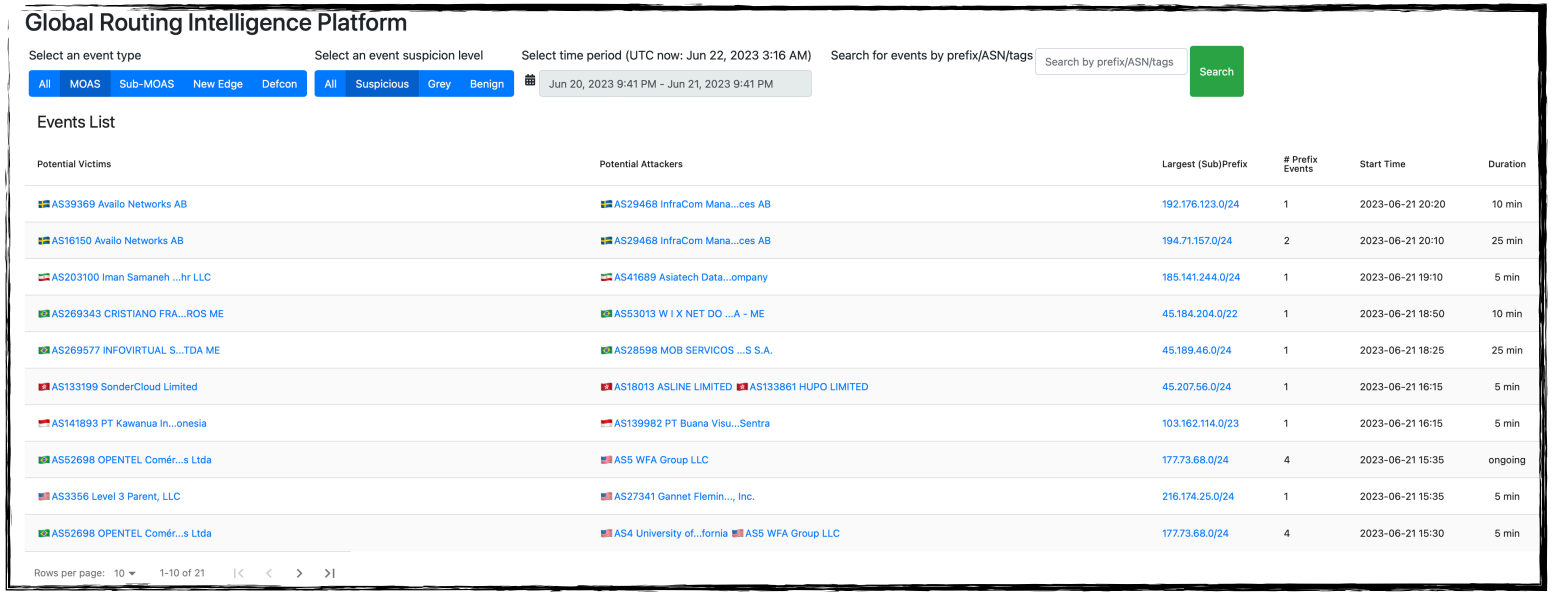
- **Hijacking**
- **Fat-finger**
- **Route Leaks**

Key question

What do we know about routing incidents?

GRIP — *https://bgp.live (grip.inetintel.cc.gatech.edu)*

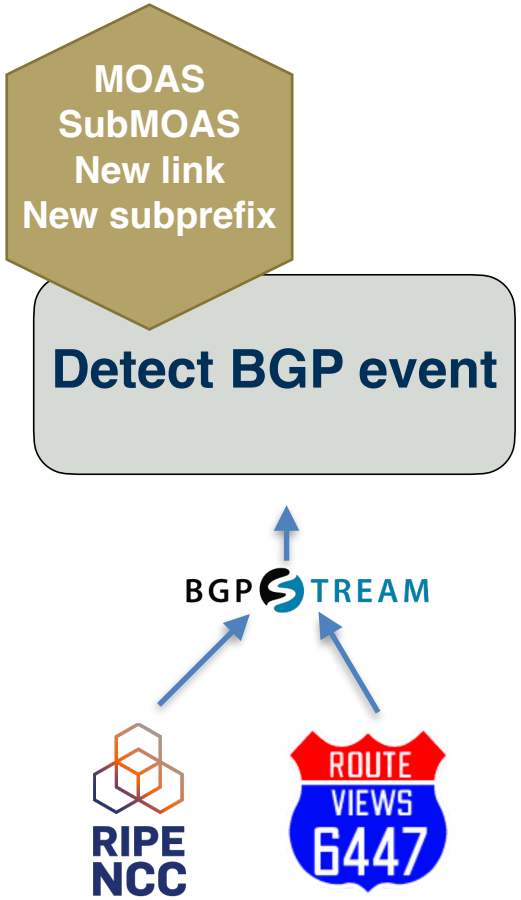
- Been around since ~2018 (CAIDA); running @ GATech since 2021
- Public dashboard + API; Open source
- Main BGP incidents datasource to the MANRS observatory
- Annotation and inference methods constantly improving
- Current status: We reprocessed the last 5 years to uncover trends



Internet Intelligence Lab

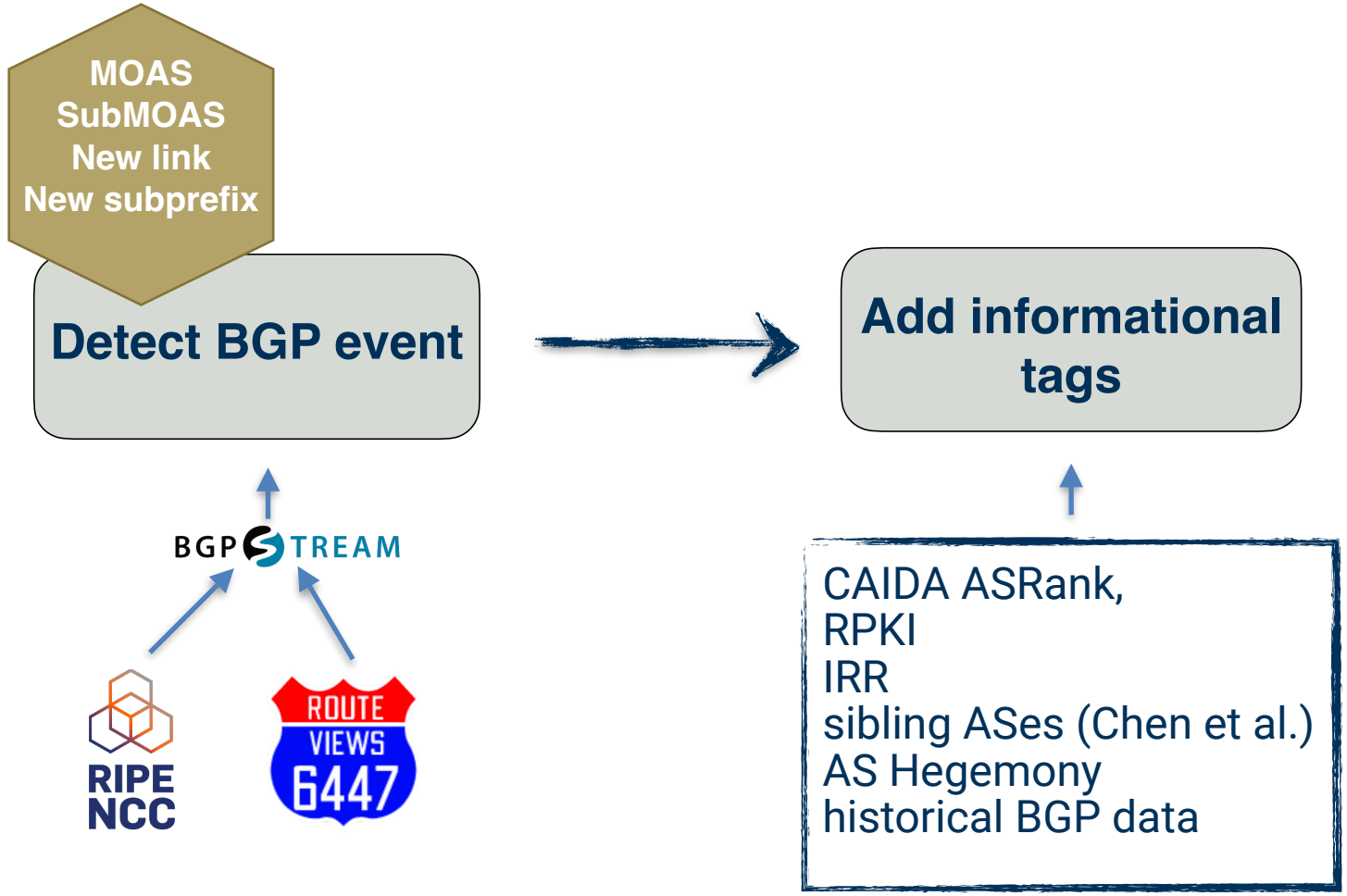
How does GRIP work?

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



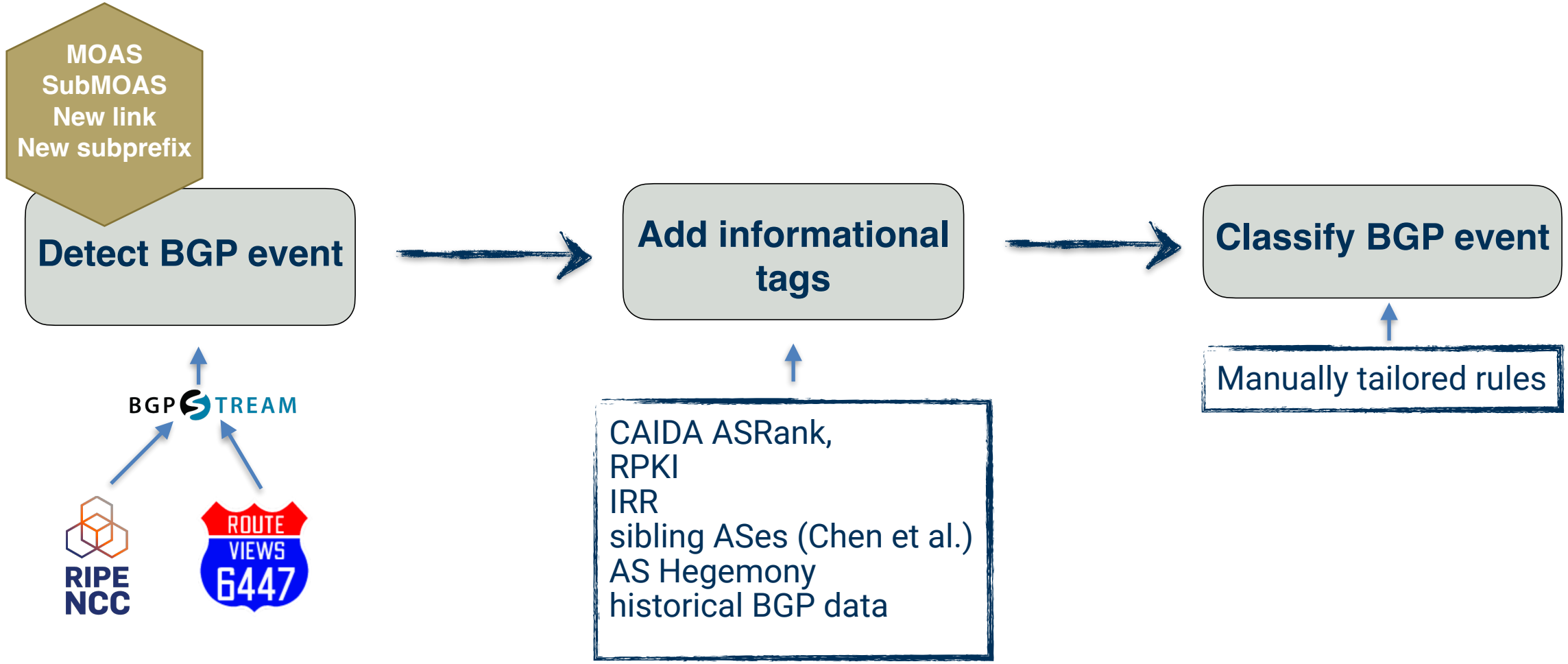
How does GRIP work?

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



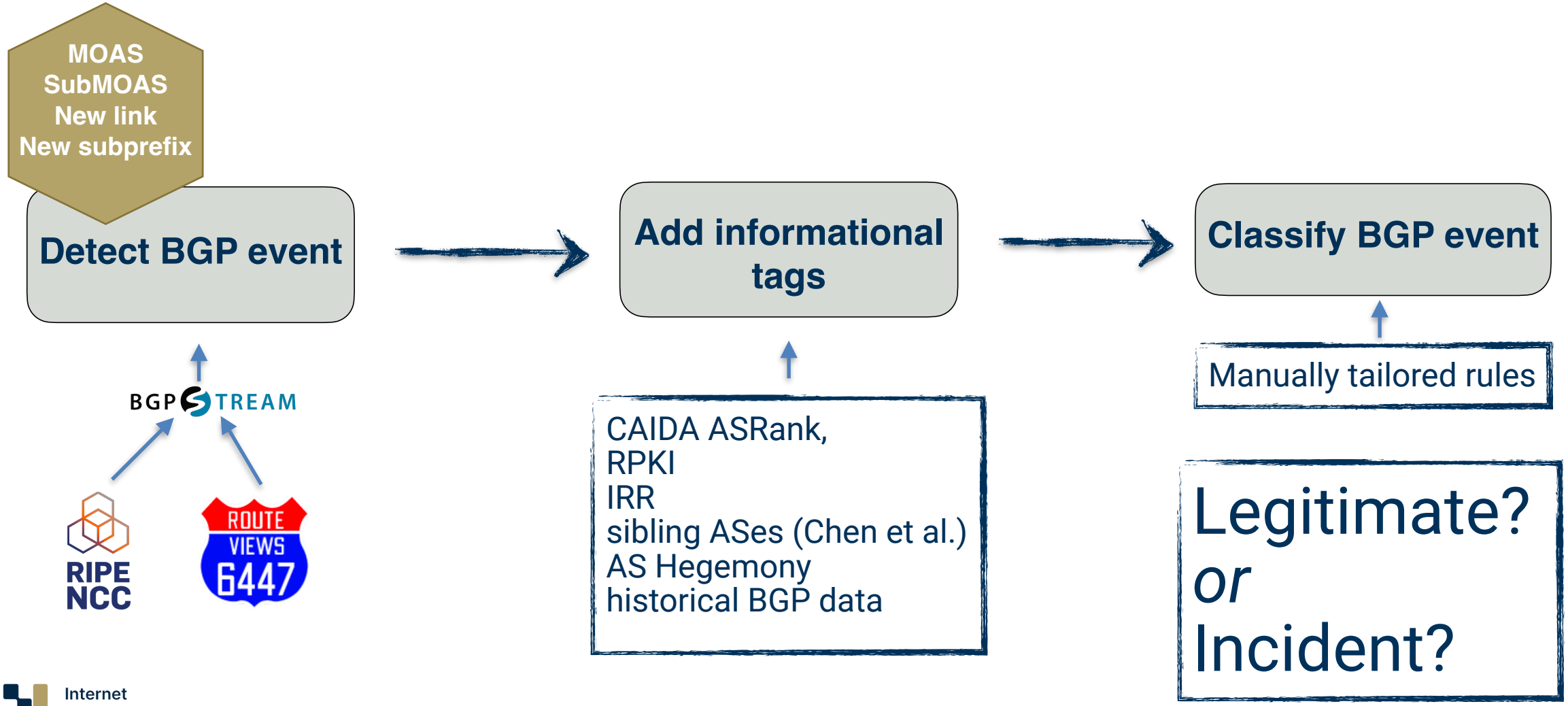
How does GRIP work?

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



How does GRIP work?

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



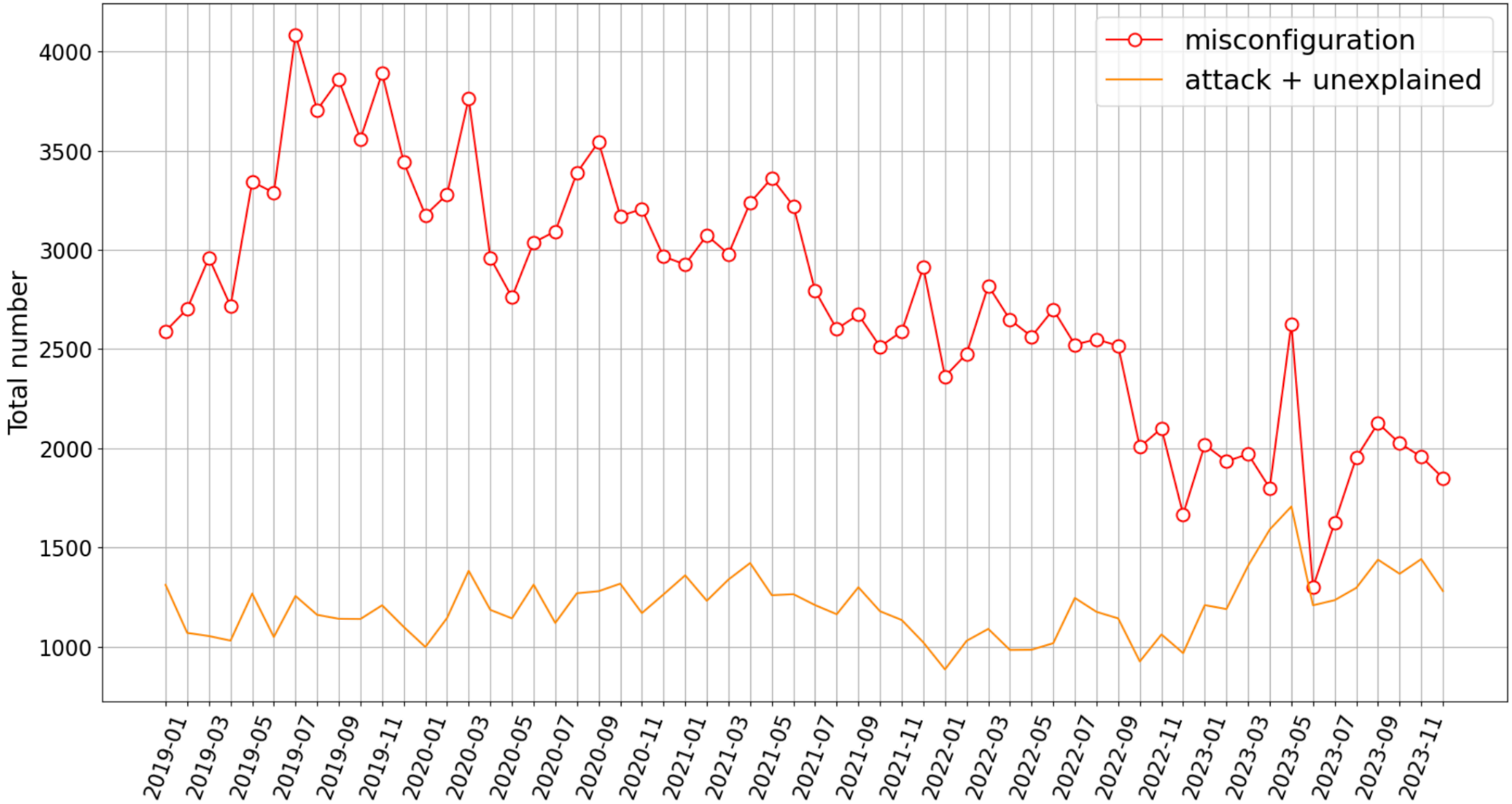
What have we observed so far?

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%]

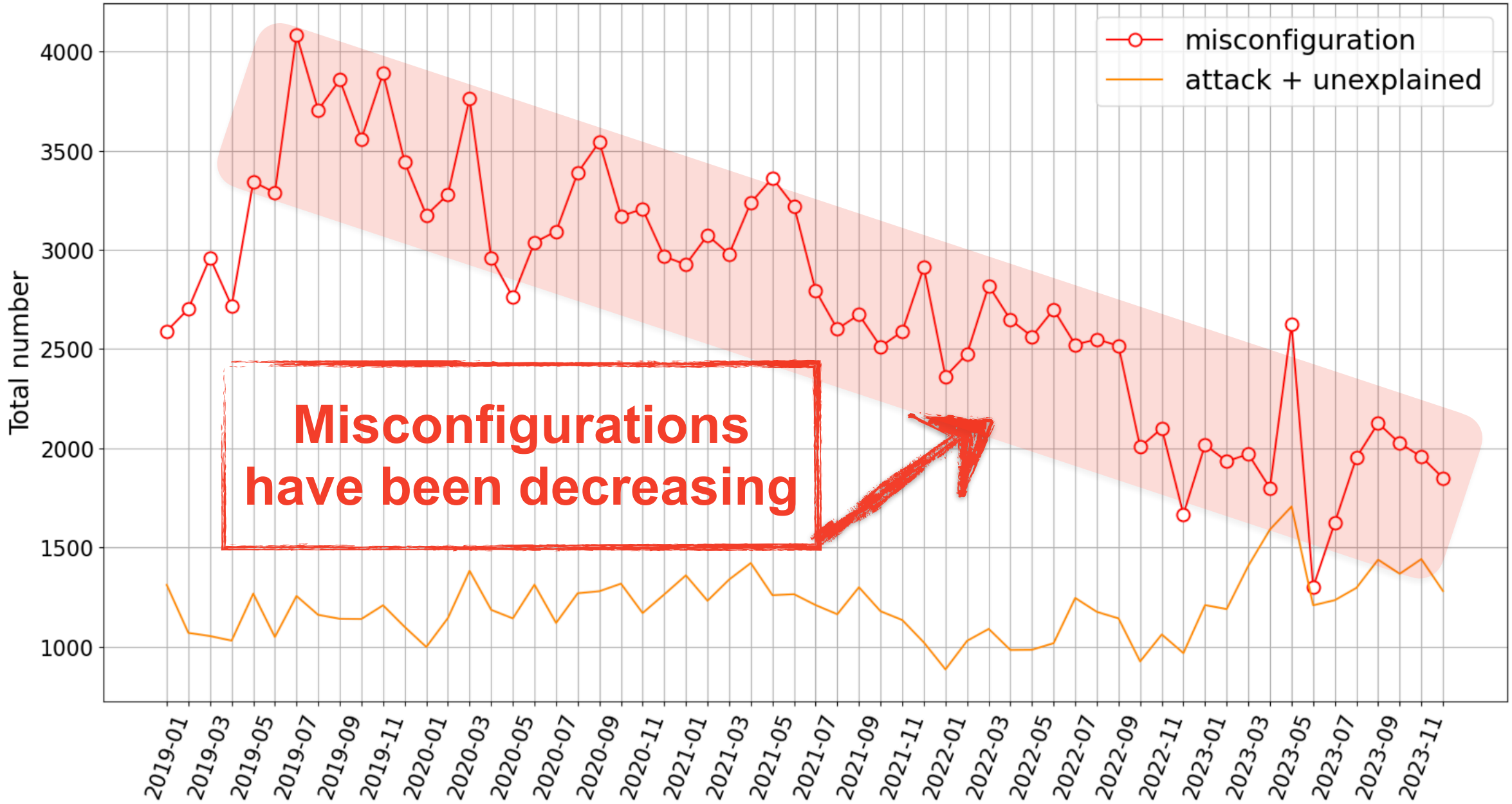
- **Legitimate 85%; ~280k/yr**
- **Incidents 15%; ~50k/yr**
  - Misconfigs 10%; 33k/yr
  - Attacks 2%; 7k/yr
  - Unexplained 2%; 7k/yr
  - Abnormal 1%; 3k/yr

Incidents



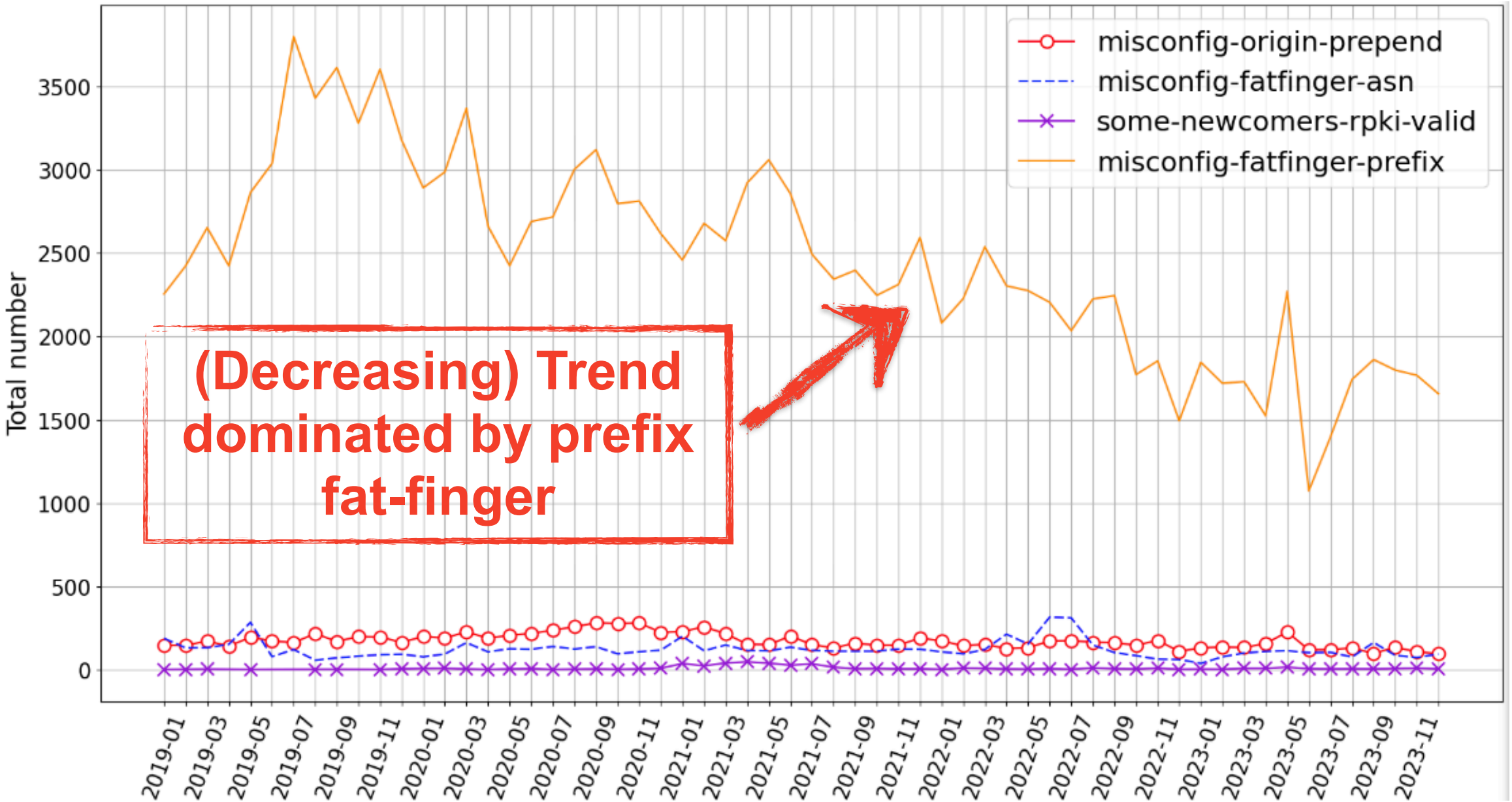
>> preliminary results <<

Incidents



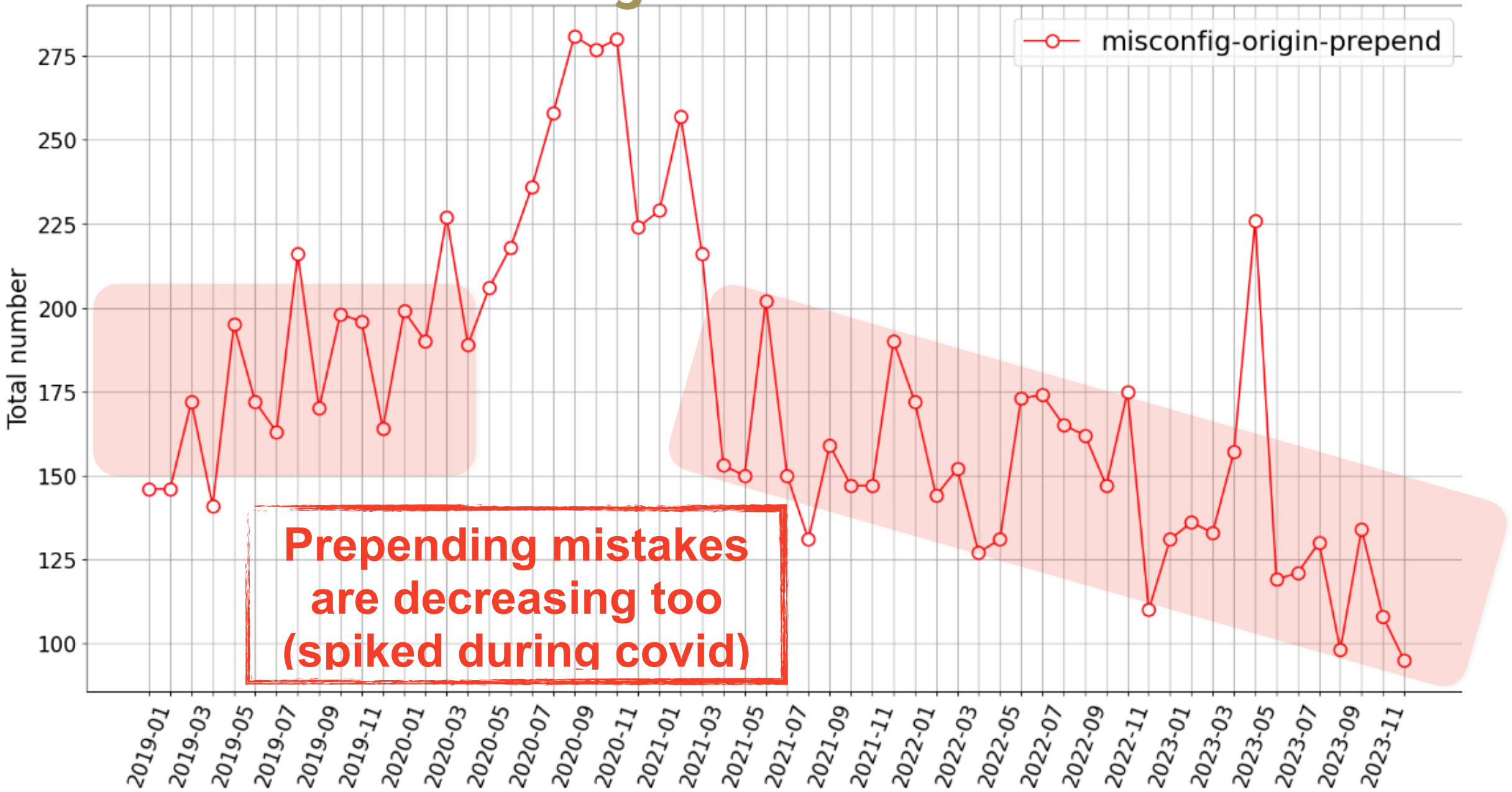
>> preliminary results <<

A closer look at misconfigurations



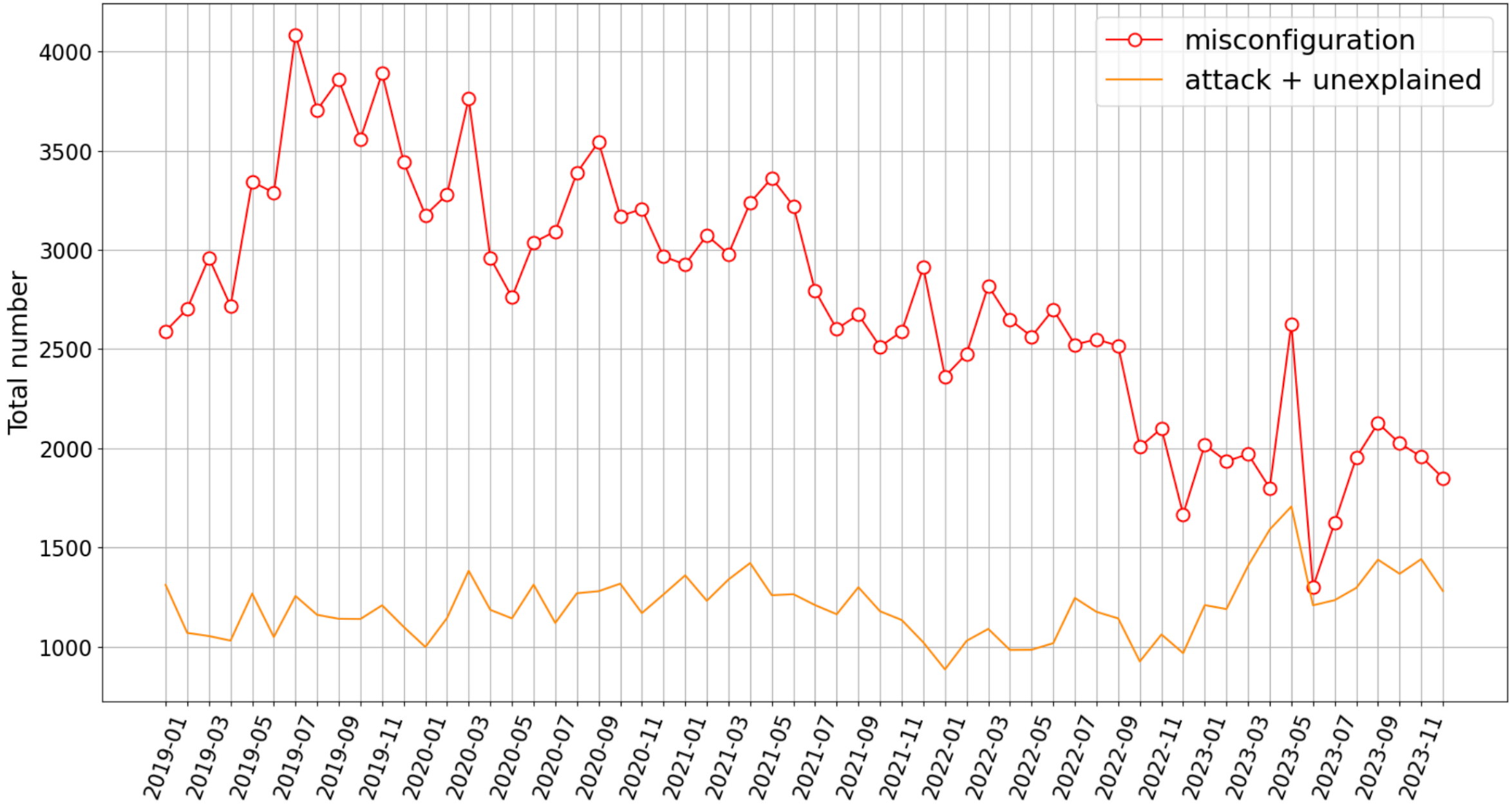
>> preliminary results <<

A closer look at misconfigurations



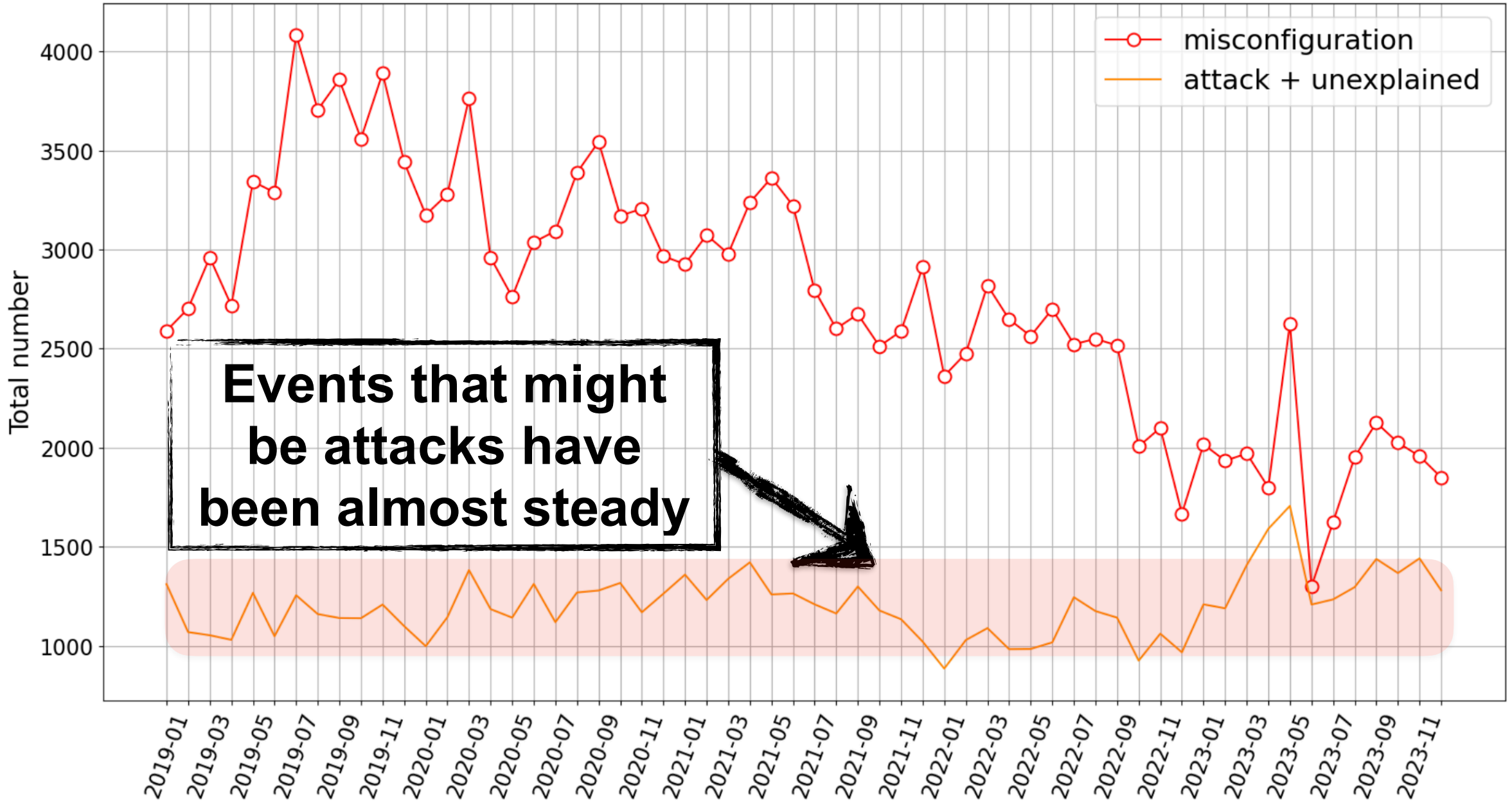
>> preliminary results <<

Incidents



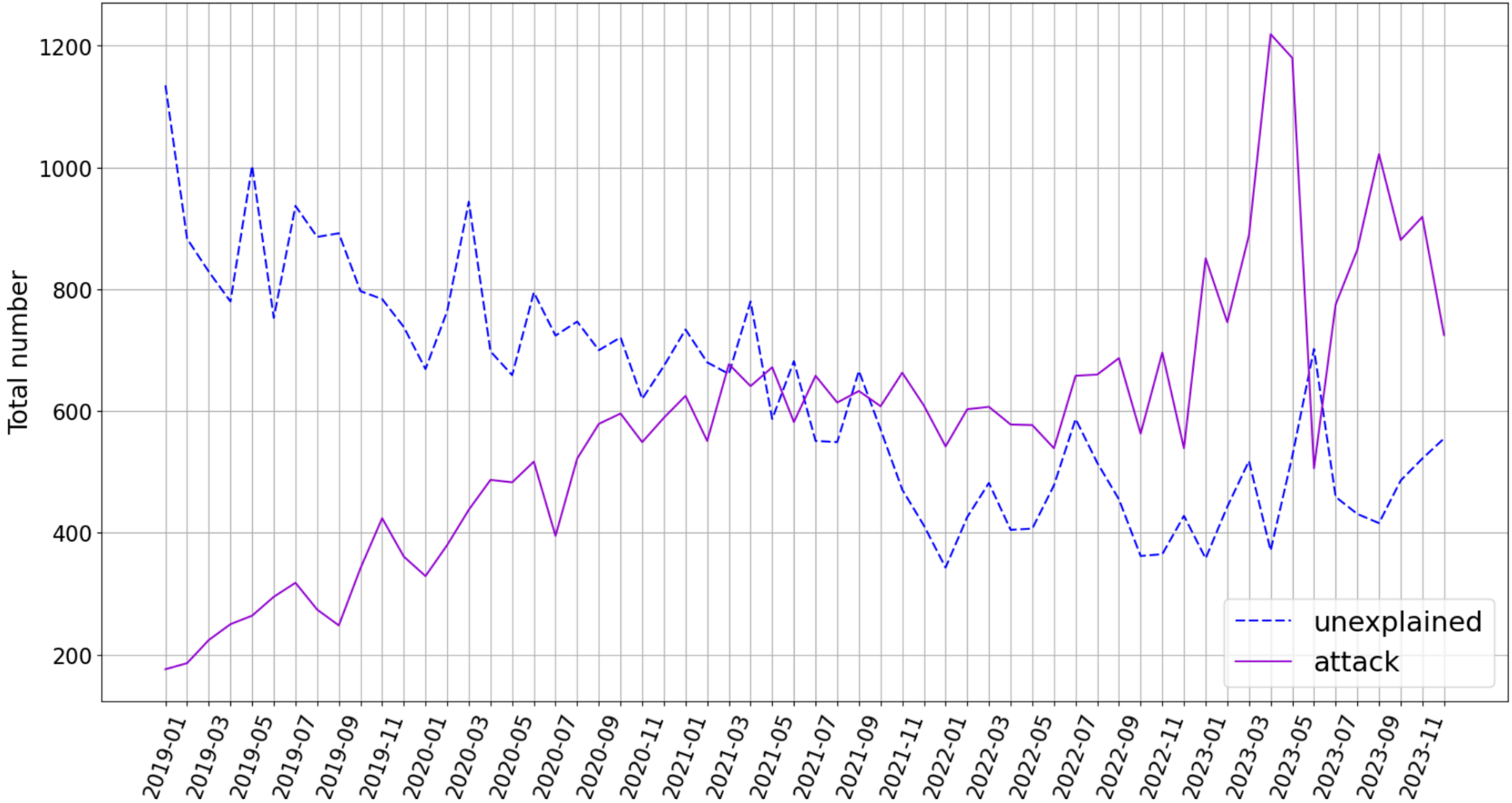
>> preliminary results <<

Incidents



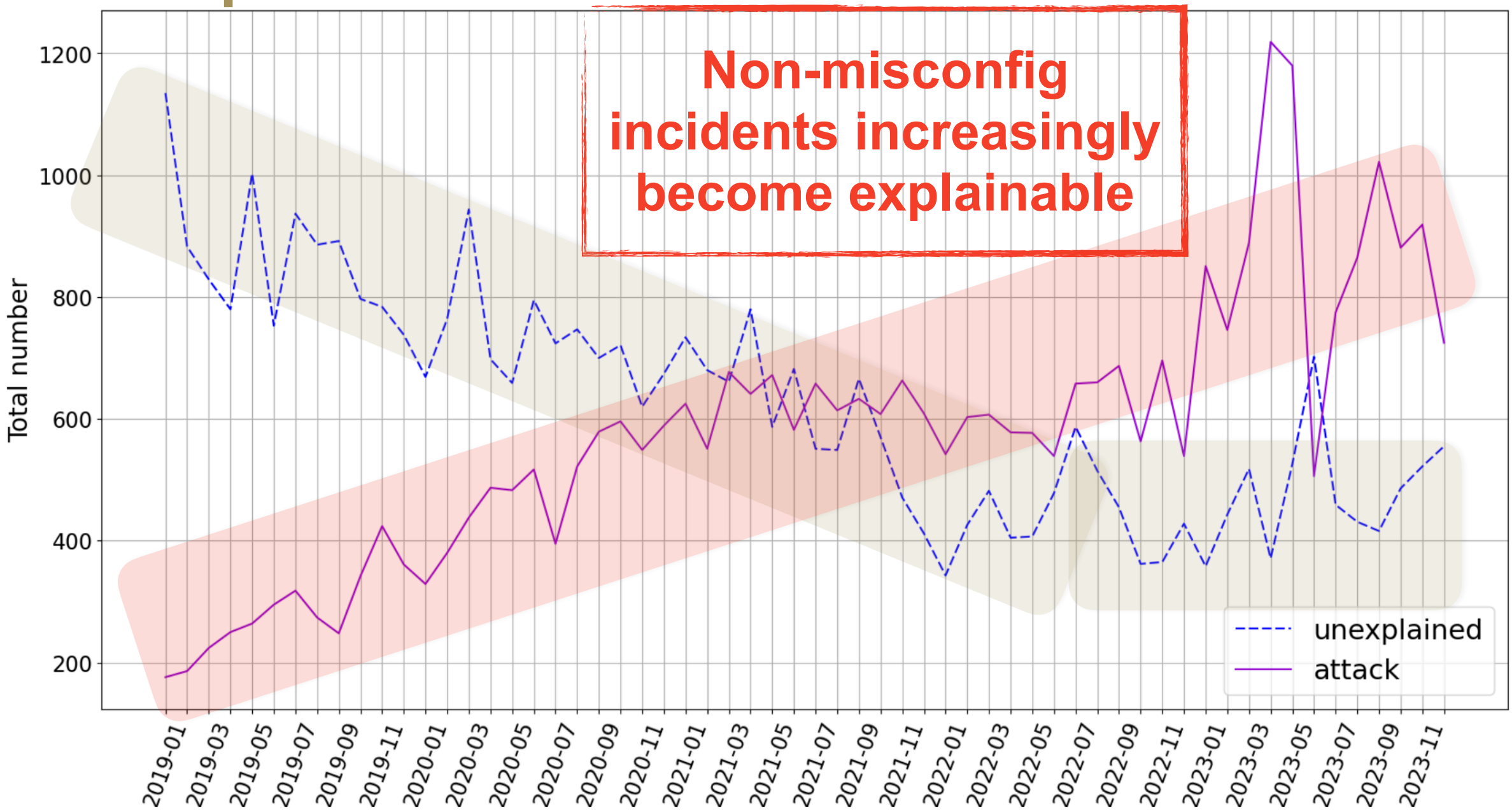
>> preliminary results <<

More “explainable” events



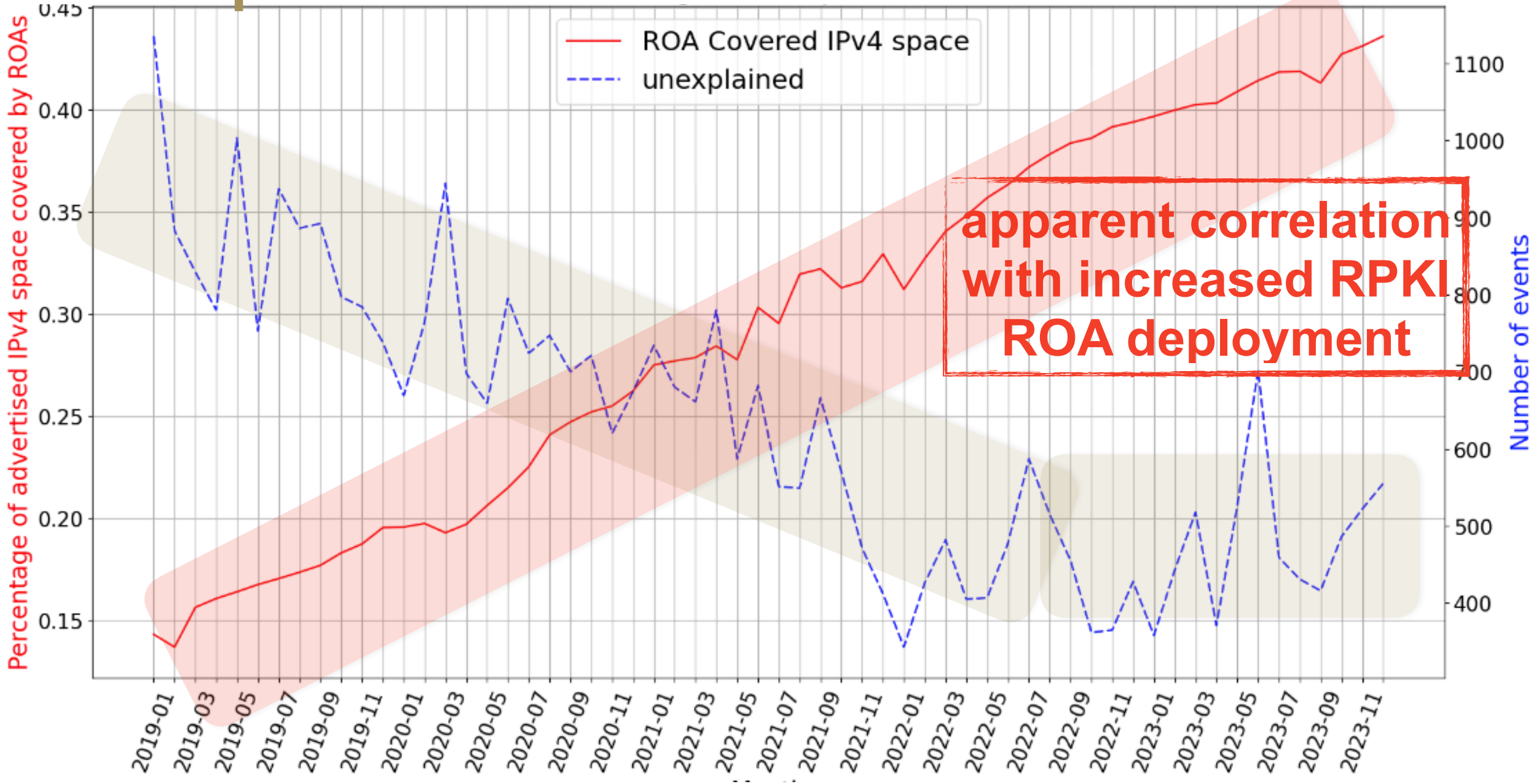
>> preliminary results <<

More “explainable” events



>> preliminary results <<

More “explainable” events



apparent correlation with increased RPKI ROA deployment

>> preliminary results <<

GRIP: How can we improve?

bgp.live

Internet Intelligence Lab

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?

bgp.live

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

- Improve reliability of operations
  - Infrastructure, developers, researchers

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!

Internet Intelligence Lab