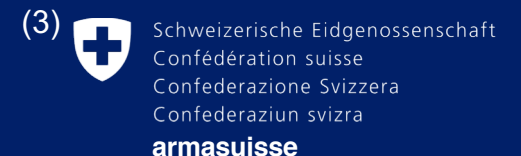
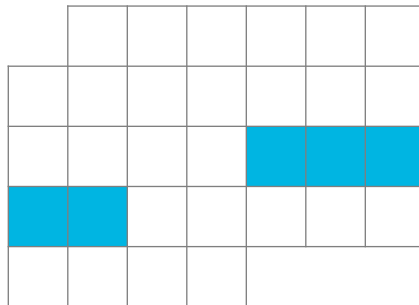


FeedRank: A Tamper-resistant Method for the Ranking of Cyber Threat Intelligence Feeds

Roland Meier⁽¹⁾, Cornelia Scherrer⁽¹⁾, David Gugelmann⁽²⁾,
Vincent Lenders⁽³⁾, Laurent Vanbever⁽¹⁾



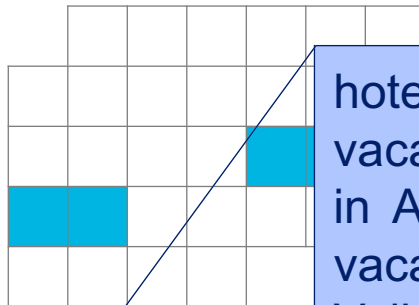


		▼

hotel in Amsterdam, flights to Amsterdam, vacation in Amsterdam, hotel in Andorra la Vella, flights to Andorra la Vella, vacation in Andorra la Vella, trip to Andorra la Vella, hotel in Ankara, flights to Ankara, vacation in Ankara, trip to Ankara, hotel in Astana, flights to Astana, vacation in Astana, trip to Astana, hotel in Athens, flights to Athens, vacation in Athens, trip to Athens, hotel in Baku, flights to Baku, vacation in Baku, trip to Baku, hotel in Belgrade, flights to Belgrade, vacation in Belgrade, trip to Belgrade, hotel in Berlin, flights to Berlin, vacation in Berlin, trip to Berlin, hotel in Bern, flights to Bern, vacation in Bern, trip to Bern, hotel in Bratislava, flights to Bratislava, vacation in Bratislava, trip to Bratislava, hotel in Brussels, flights to Brussels, vacation in Brussels, trip to Brussels, hotel in Bucharest, flights to Bucharest, vacation in Bucharest, trip to Bucharest, hotel in Budapest, flights to Budapest, vacation in Budapest, trip to Budapest, hotel in Chişinău, flights to Chişinău, vacation in Chişinău, trip to Chişinău, hotel in Copenhagen, flights to Copenhagen, vacation in Copenhagen, trip to Copenhagen, hotel in Dublin, flights to Dublin, vacation in Dublin, trip to Dublin, hotel in Helsinki, flights to Helsinki, vacation in Helsinki, trip to Helsinki, hotel in Kiev, flights to Kiev, vacation in Kiev, trip to Kiev, hotel in Lisbon, flights to Lisbon, vacation in Lisbon, trip to Lisbon, hotel in Ljubljana, flights to Ljubljana, vacation in Ljubljana, trip to Ljubljana, hotel in London, flights to London, vacation in London, trip to London, hotel in Luxembourg, flights to Luxembourg, vacation in Luxembourg, trip to Luxembourg, hotel in Madrid, flights to Madrid, vacation in Madrid, trip to Madrid, hotel in Minsk, flights to Minsk, vacation in Minsk, trip to Minsk, hotel in Monaco, flights to Monaco, vacation in Monaco, trip to Monaco, hotel in Moscow, flights to Moscow, vacation in Moscow, trip to Moscow, hotel in Nicolaș, flights to Nicolaș, vacation in Nicolaș, trip to Nicolaș, hotel in Oslo, flights to Oslo, vacation in Oslo, trip to Oslo, hotel in Paris, flights to Paris, vacation in Paris, trip to Paris, hotel in Podgorica, flights to Podgorica, vacation in Podgorica, trip to Podgorica, hotel in Prague, flights to Prague, vacation in Prague, trip to Prague, hotel in Pristina, flights to Pristina, vacation in Pristina, trip to Pristina, hotel in Reykjavík, flights to Reykjavík, vacation in Reykjavík, trip to Reykjavík, hotel in Riga, flights to Riga, vacation in Riga, trip to Riga, hotel in Rome, flights to Rome, vacation in Rome, trip to Rome, hotel in San Marino, flights to San Marino, vacation in San Marino, trip to San Marino, hotel in Sarajevo, flights to Sarajevo, vacation in Sarajevo, trip to Sarajevo, hotel in Skopje, flights to Skopje, vacation in Skopje, trip to Skopje, hotel in Sofia, flights to Sofia, vacation in Sofia, trip to Sofia, hotel in Stockholm, flights to Stockholm, vacation in Stockholm, trip to Stockholm, hotel in Tallinn, flights to Tallinn, vacation in Tallinn, trip to Tallinn, hotel in Tbilisi, flights to Tbilisi, vacation in Tbilisi, trip to Tbilisi, hotel in Tirana, flights to Tirana, vacation in Tirana, trip to Tirana, hotel in Vaduz, flights to Vaduz, vacation in Vaduz, trip to Vaduz, hotel in Valletta, flights to Valletta, vacation in Valletta, trip to Valletta, hotel in Vatican City, flights to Vatican City, vacation in Vatican City, trip to Vatican City, hotel in Vienna, flights to Vienna, vacation in Vienna, trip to Vienna, hotel in Vilnius, flights to Vilnius, vacation in Vilnius, trip to Vilnius, hotel in Warsaw, flights to Warsaw, vacation in Warsaw, trip to Warsaw, hotel in Yerevan, flights to Yerevan, vacation in Yerevan, trip to Yerevan, hotel in Zagreb, flights to Zagreb, vacation in Zagreb, trip to Zagreb



```
<meta name="keywords" content="flights to  
Bern, vacation in Bern, trip to Bern, hotel  
in Bratislava, flights to Bratislava,  
vacation in Bratislava, trip to Bratislava,  
hotel in Brussels, flights to Brussels,  
vacation in Brussels" />
```

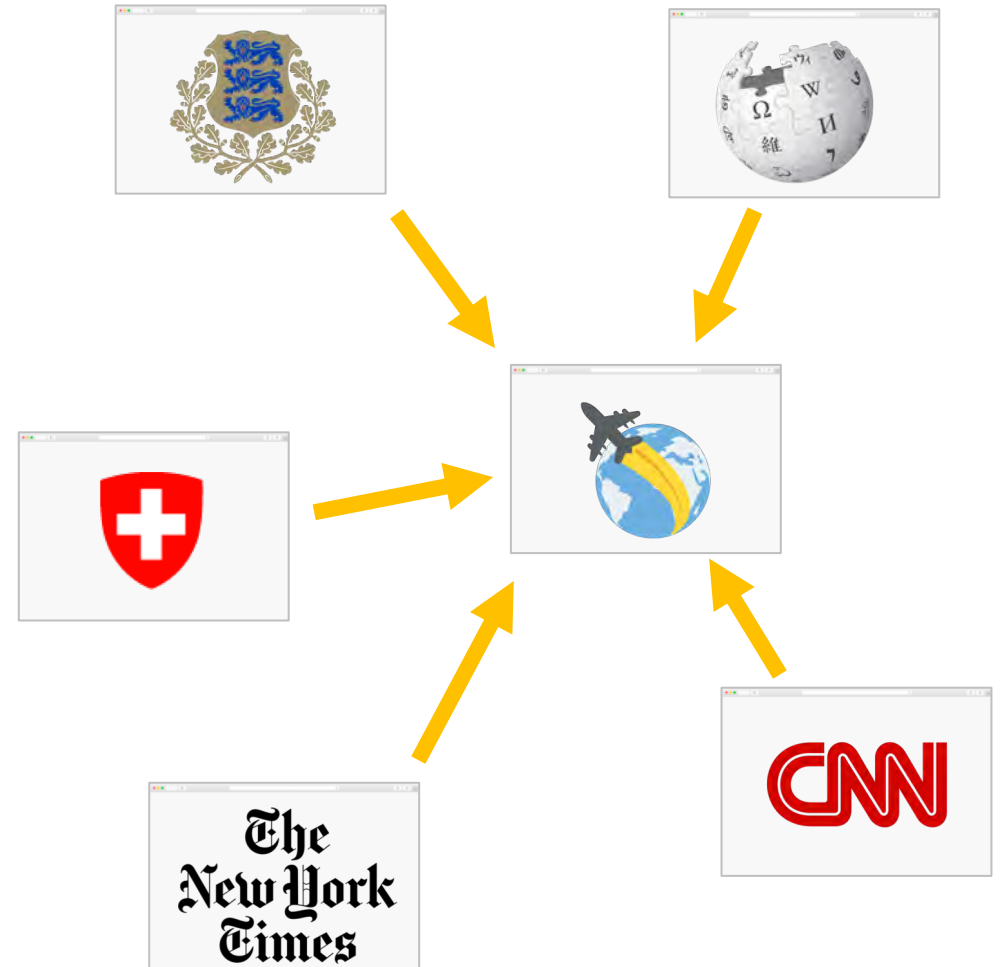


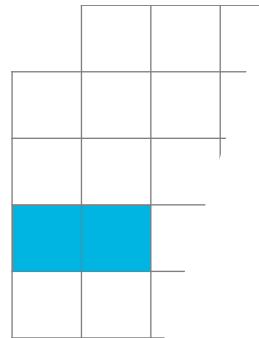
hotel in Amsterdam, flights to Amsterdam, vacation in Amsterdam, trip to Amsterdam, hotel in Andorra la Vella, flights to Andorra la Vella, vacation in Andorra la Vella, trip to Andorra la Vella, hotel in Ankara, flights to Ankara, vacation in Ankara, trip to Ankara, hotel in Astana, flights to Astana, vacation in Astana, trip to Astana

<p>hotel in Amsterdam, flights to Amsterdam, vacation in Amsterdam</p> <p>hotel in Astana, flights to Astana, vacation in Astana</p> <p>hotel in Berlin, flights to Berlin, vacation in Berlin</p> <p>hotel in Bucharest, flights to Bucharest, vacation in Bucharest</p> <p>hotel in Copenhagen, flights to Copenhagen, vacation in Copenhagen</p> <p>hotel in Lisbon, flights to Lisbon, vacation in Lisbon</p> <p>hotel in Madrid, flights to Madrid, vacation in Madrid</p> <p>hotel in Moscow, flights to Moscow, vacation in Moscow</p> <p>hotel in Podgorica, flights to Podgorica, vacation in Podgorica</p> <p>hotel in Riga, flights to Riga, vacation in Riga</p> <p>hotel in Skopje, flights to Skopje, vacation in Skopje</p> <p>hotel in Tbilisi, flights to Tbilisi, vacation in Tbilisi</p> <p>hotel in Vatican City, flights to Vatican City, vacation in Vatican City</p> <p>hotel in Warsaw, flights to Warsaw, vacation in Warsaw</p>	<p>hotel in Andorra la Vella, flights to Andorra la Vella, vacation in Andorra la Vella</p> <p>hotel in Athens, flights to Athens, vacation in Athens</p> <p>hotel in Bern, flights to Bern, vacation in Bern</p> <p>hotel in Budapest, flights to Budapest, vacation in Budapest</p> <p>hotel in Dublin, flights to Dublin, vacation in Dublin</p> <p>hotel in Ljubljana, flights to Ljubljana, vacation in Ljubljana</p> <p>hotel in Minsk, flights to Minsk, vacation in Minsk</p> <p>hotel in Nicosia, flights to Nicosia, vacation in Nicosia</p> <p>hotel in Oslo, flights to Oslo, vacation in Oslo</p> <p>hotel in Pristina, flights to Pristina, vacation in Pristina</p> <p>hotel in Reykjavik, flights to Reykjavik, vacation in Reykjavik</p> <p>hotel in San Marino, flights to San Marino, vacation in San Marino</p> <p>hotel in Sofia, flights to Sofia, vacation in Sofia</p> <p>hotel in Stockholm, flights to Stockholm, vacation in Stockholm</p> <p>hotel in Tirana, flights to Tirana, vacation in Tirana</p> <p>hotel in Vienna, flights to Vienna, vacation in Vienna</p> <p>hotel in Zareeb, flights to Zareeb, vacation in Zareeb</p>	<p>in Ankara, trip to Ankara, hotel in Ankara</p> <p>to Astana, vacation in Astana</p>
---	---	--

Ranking Websites

- Websites can contain arbitrary content
- Websites can contain links *to* any other website
- **PageRank:** A website *to which* many other websites refer to is likely to be important





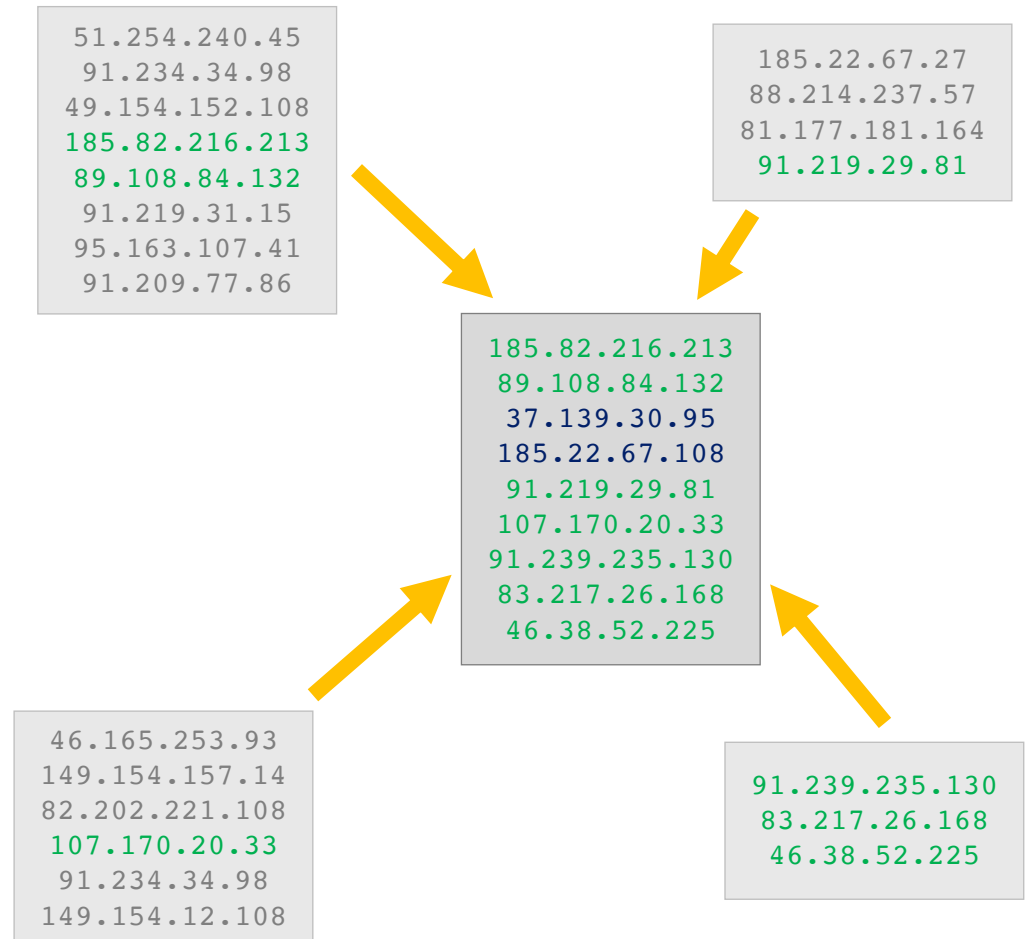
hotel in Amsterdam, flights to Amsterdam, vacation in Amsterdam, trip to Amsterdam, hotel in Andorra, Ankara, trip to Ankara, hotel in Astana, flights to Astana, vacation in Astana, trip to Astana, hotel in Ałaj flights to Belgrade, vacation in Belgrade, trip to Belgrade, hotel in Berlin, flights to Berlin, vacation in Bratislava, trip to Bratislava, hotel in Brussels, flights to Brussels, vacation in Brussels, trip to Brus Budapest, trip to Budapest, hotel in Chişinău, flights to Chişinău, vacation in Chişinău, trip to Chişinău Dublin, trip to Dublin, hotel in Helsinki, flights to Helsinki, vacation in Helsinki, trip to Helsinki, hotel to Ljubljana, vacation in Ljubljana, trip to Ljubljana, hotel in London, flights to London, vacation in Madrid, vacation in Madrid, trip to Madrid, hotel in Minsk, flights to Minsk, vacation in Minsk, trip to Moscow, hotel in Nicosia, flights to Nicosia, vacation in Nicosia, trip to Nicosia, hotel in Podgorica, vacation in Podgorica, trip to Podgorica, hotel in Prague, flights to Prague, vacation in Reykjavík, trip to Reykjavík, hotel in Riga, flights to Riga, vacation in Riga, trip to Riga, hotel in Sarajevo, flights to Sarajevo, vacation in Sarajevo, trip to Sarajevo, hotel in Skopje, flights to Skopje, vacation in Stockholm, trip to Stockholm, hotel in Tallinn, flights to Tallinn, vacation in Tallinn hotel in Vaduz, flights to Vaduz, vacation in Vaduz, trip to Vaduz, hotel in Valletta, flights to Valletta

The image features a background of a sunset over a body of water, with a large, semi-transparent blue triangle overlaid on the right side. Inside the triangle, there is a grid of IP addresses in a dark blue font. The text "... to Cyber Threat Intelligence Feeds" is overlaid on the bottom right of the triangle in a large, bold, dark blue font.

...to Cyber Threat Intelligence Feeds

Ranking Cyber Threat Intelligence Feeds

- Feeds can contain arbitrary entries
- Feeds can copy entries from any other feed
- FeedRank:** A feed whose entries are confirmed by other feeds is likely to be of high quality



FeedRank

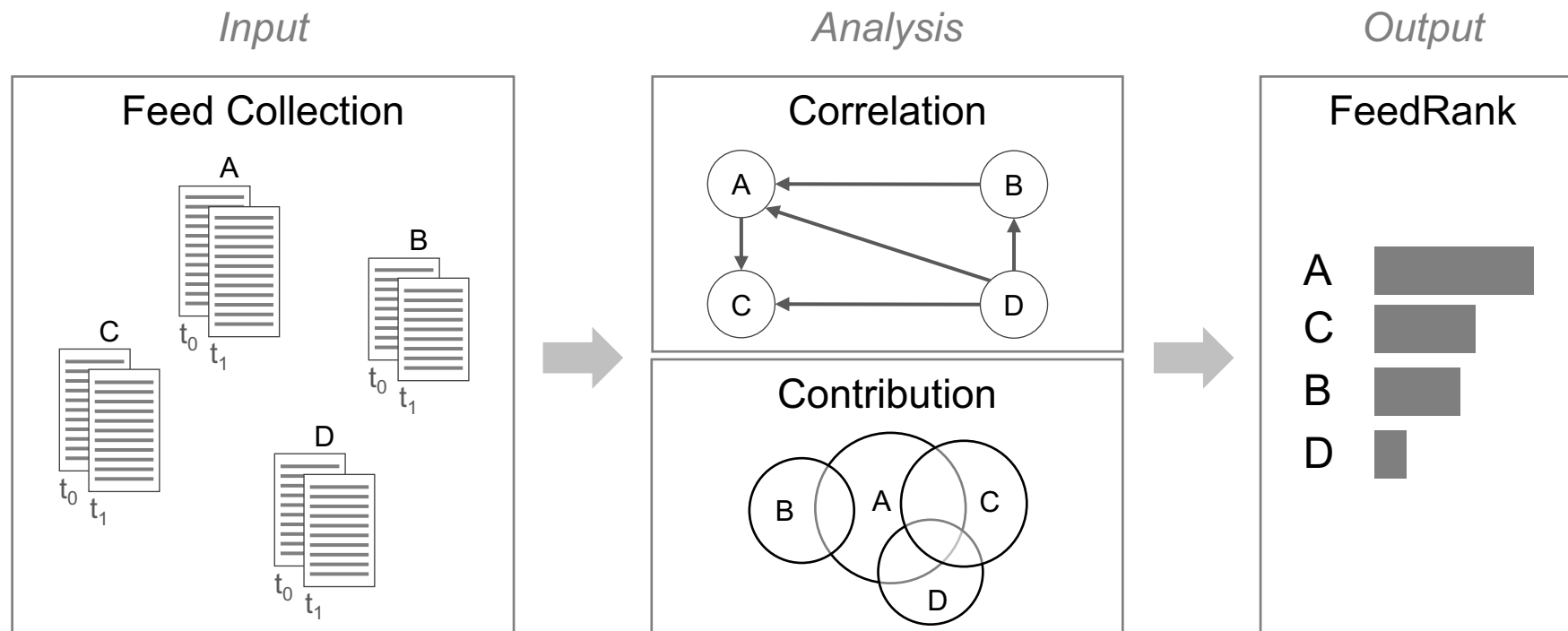
Evaluate cyber threat intelligence feeds in a way that

- Allows us to identify high quality feeds
- Is customizable for different preferences of network defenders
- Does not require a ground truth
- Scales to the large ecosystem of feeds
- Is robust against dishonest feed providers

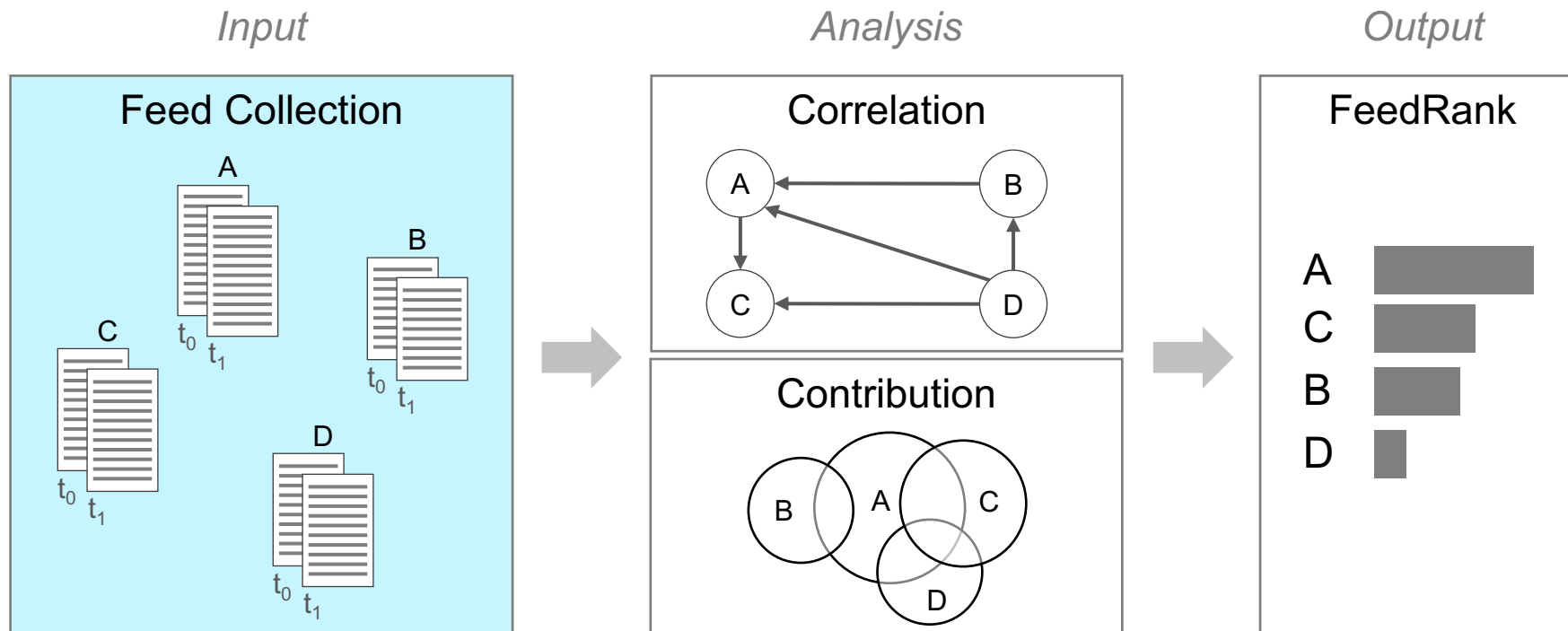
Properties of High Quality Feeds

- **Completeness** Contain all malicious endpoints
- **Accuracy** Do not list benign endpoints
- **Speed** Be complete and accurate upon changes

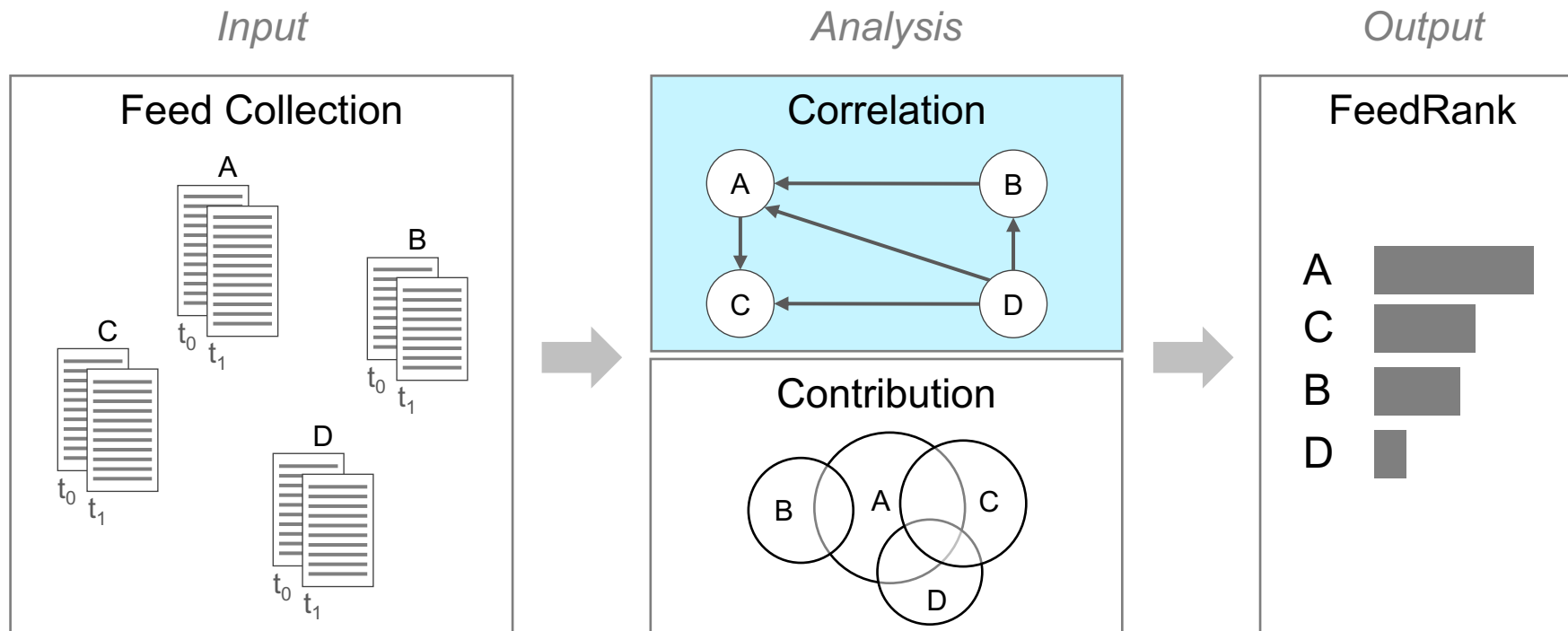
FeedRank Operates in 3 Steps



Step 1: Collect Feed Data



Step 2a: Analyze Correlations Between Feeds



Step 2a: Analyze Correlations Between Feeds

- Correlation Graph: Directed graph with
 - vertices \leftarrow feeds
 - edges \leftarrow correlations

Step 2a: Analyze Correlations Between Feeds

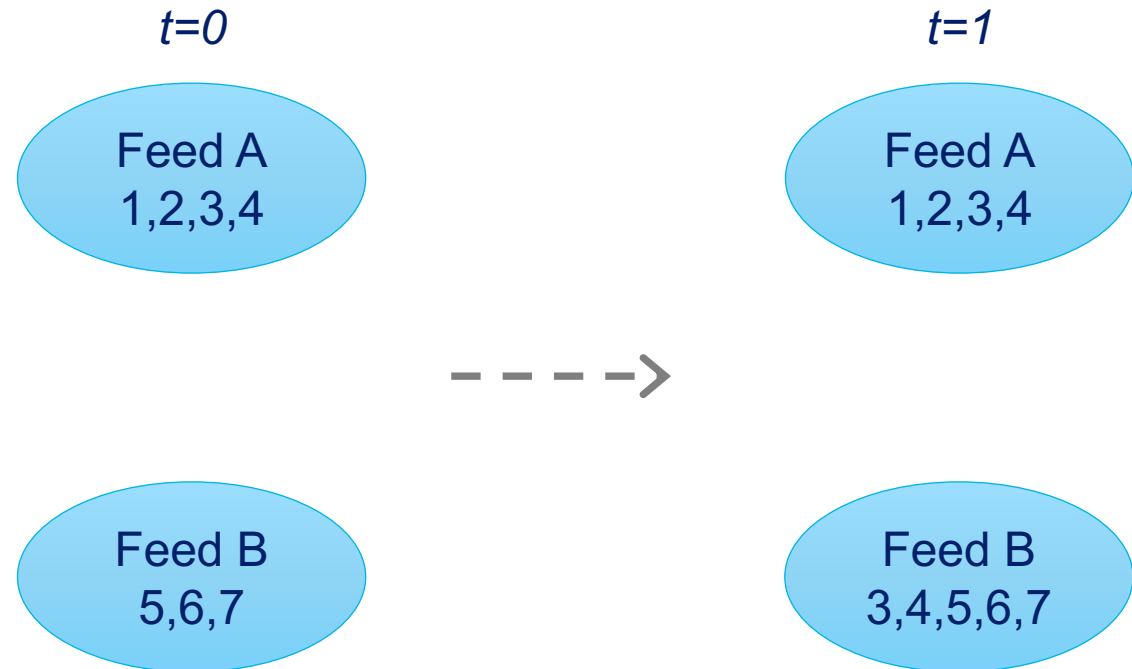
- Correlation Graph: Directed graph with
 - vertices \leftarrow feeds
 - edges \leftarrow correlations

$t=0$



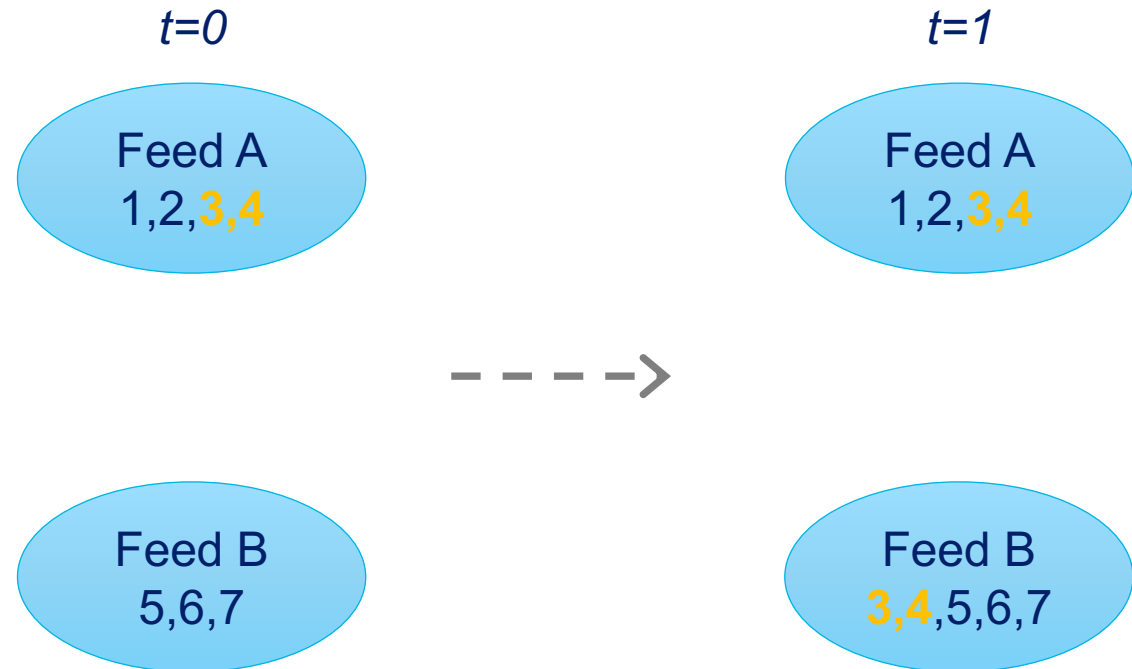
Step 2a: Analyze Correlations Between Feeds

- Correlation Graph: Directed graph with
 - vertices \leftarrow feeds
 - edges \leftarrow correlations



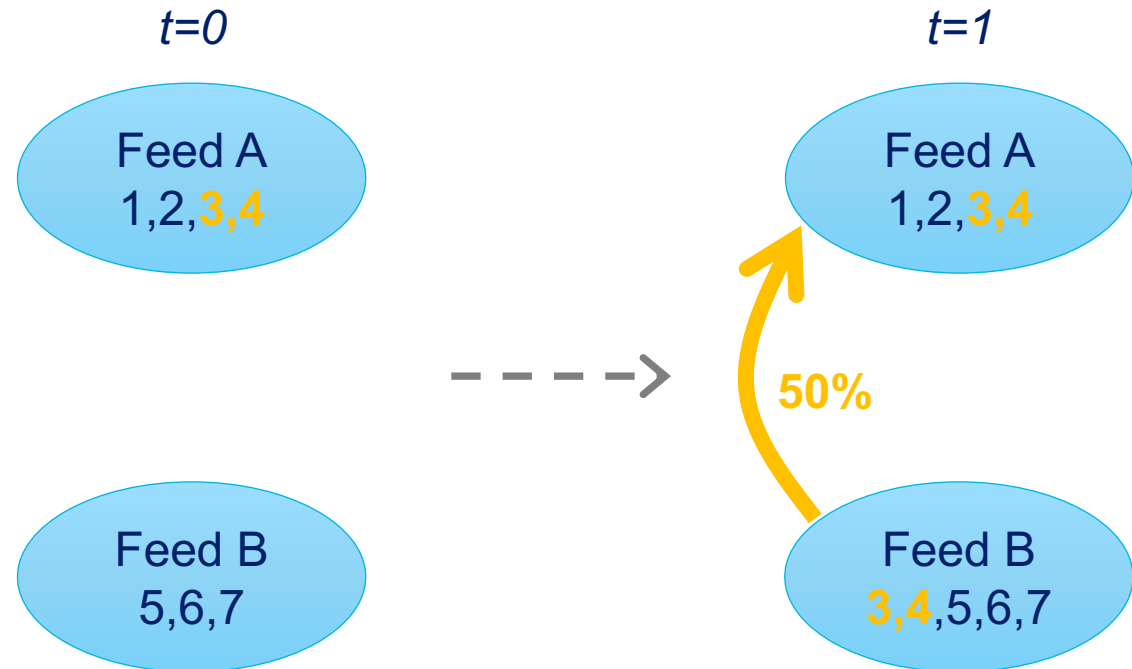
Step 2a: Analyze Correlations Between Feeds

- Correlation Graph: Directed graph with
 - vertices \leftarrow feeds
 - edges \leftarrow correlations

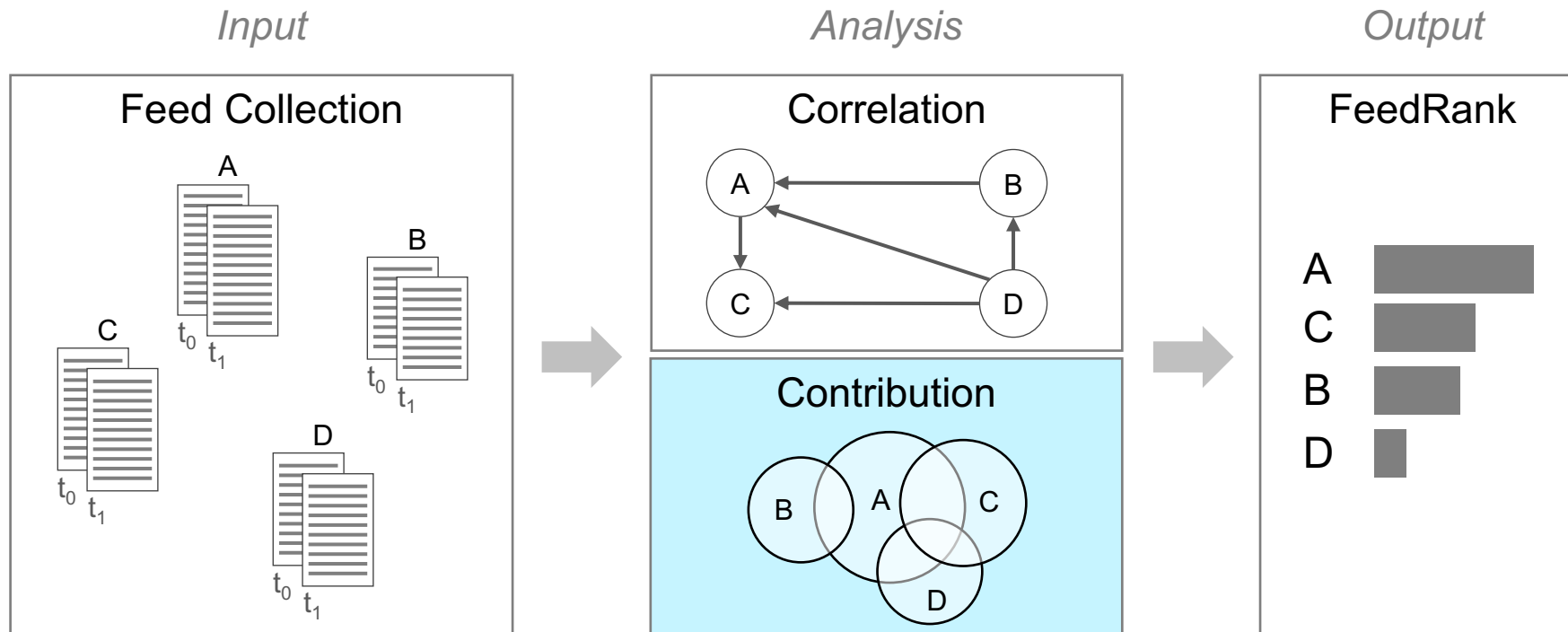


Step 2a: Analyze Correlations Between Feeds

- Correlation Graph: Directed graph with
 - vertices \leftarrow feeds
 - edges \leftarrow correlations



Step 2b: Determine the Contribution of Each Feed



Step 2b: Determine the Contribution of Each Feed

- Measure the percentage of entries that originated from each feed

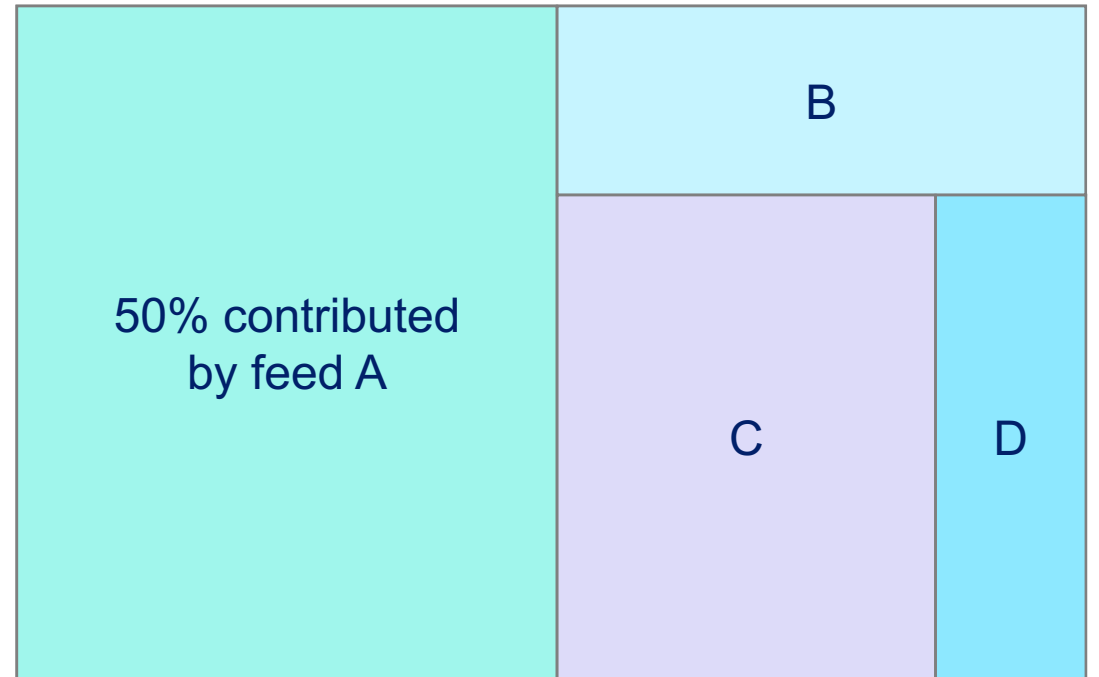
Step 2b: Determine the Contribution of Each Feed

- Measure the percentage of entries that originated from each feed

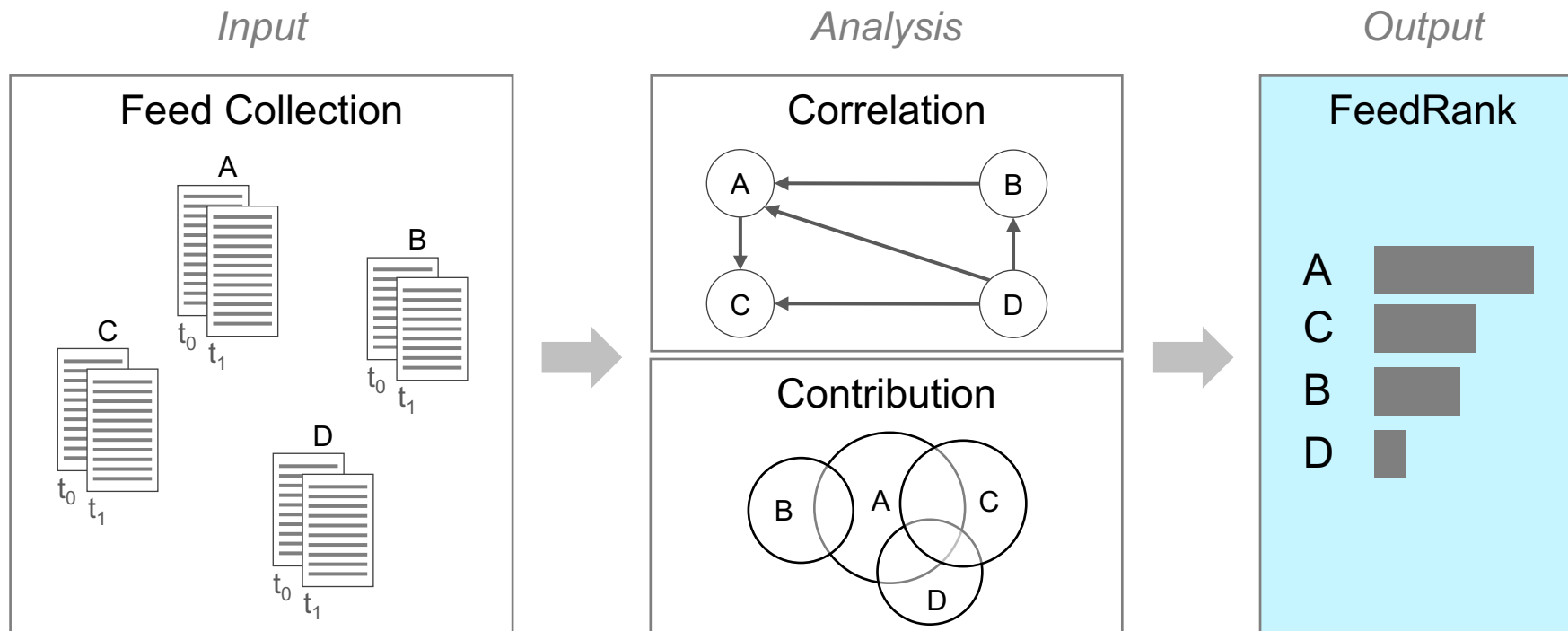
All listed endpoints (IPs)

Step 2b: Determine the Contribution of Each Feed

- Measure the percentage of entries that originated from each feed



Step 3: Compute a Ranking



Properties of High Quality Feeds

- **Completeness** Contain all malicious endpoints
 - Contribution analysis
- **Accuracy** Do not list benign endpoints
 - Correlation analysis (edge weights)
- **Speed** Be complete and accurate upon changes
 - Correlation analysis (edge directions)


FeedRank is robust against dishonest feed providers

Tampering strategies:

- Add entries
- Remove entries
- Replace entries



FeedRank is robust against dishonest feed providers

Tampering strategies:

- Add entries
 - Remove entries
 - Replace entries
-  Random entries are not confirmed by other feeds;
Copied entries appear on other feeds first




FeedRank is robust against dishonest feed providers

Tampering strategies:

- Add entries  Random entries are not confirmed by other feeds;
Copied entries appear on other feeds first
- Remove entries  Removing confirmed entries results in a lower score;
Removing unconfirmed entries truly improves the feed's quality
- Replace entries

FeedRank is robust against dishonest feed providers

Tampering strategies:

- Add entries  Random entries are not confirmed by other feeds;
Copied entries appear on other feeds first
- Remove entries  Removing confirmed entries results in a lower score;
Removing unconfirmed entries truly improves the feed's quality
- Replace entries  Combination of the above

Evaluation

- Contribution analysis



- FeedRank vs. individual metrics

- Tamper-resistance



- Case-study: Find the the best feeds w.r.t. completeness

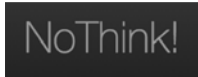
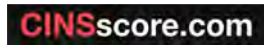


- Case-study: Find the fastest feeds

Dataset

Real feeds

- 27 freely available IP feeds
- Between 20 and ~50k entries



Dishonest feeds



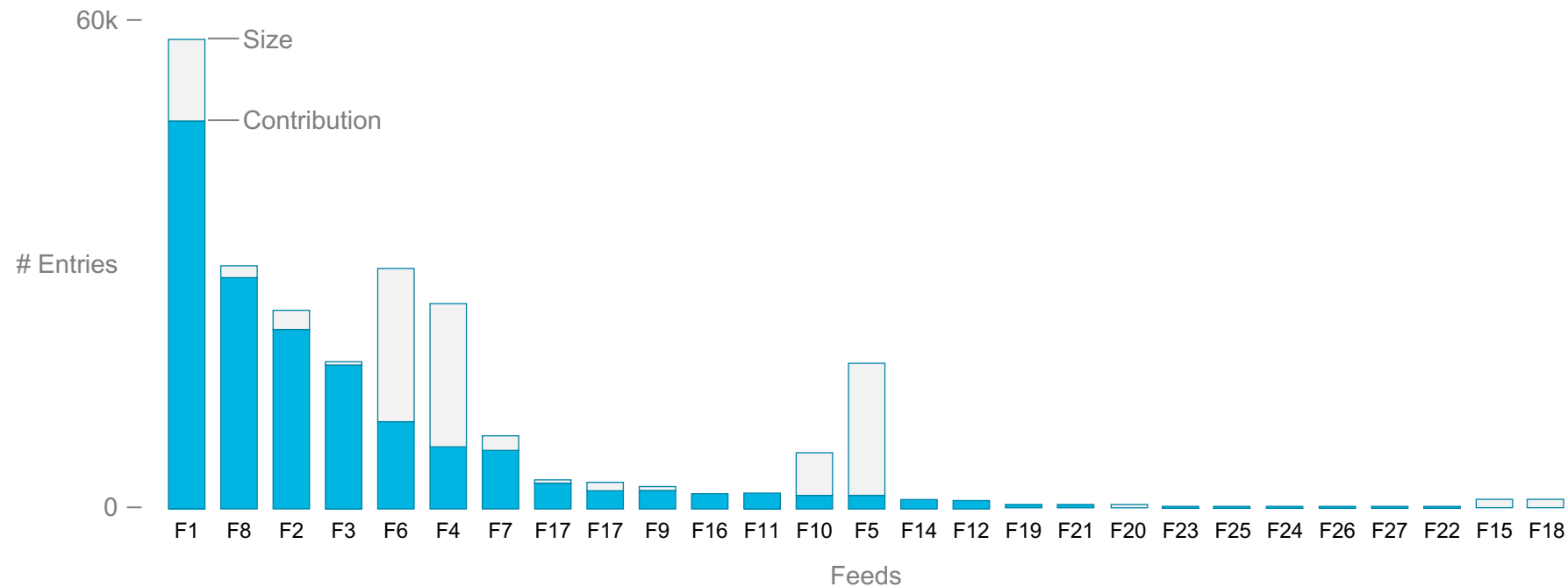
- *RandomFeed*
contains 50k random IPs



- *CopyFeed*
copies entries from the two best real feeds

5 Feeds Contribute 80% of the IPs

But a feed's size is not a good indicator of contribution.



Tamper-resistance

Dishonest feeds can cheat with individual metrics, but not with FeedRank.

- Size
- Update rate

Tamper-resistance

Dishonest feeds can cheat with individual metrics, but not with FeedRank.

Individual metrics



RandomFeed



CopyFeed



Tamper-resistance

Dishonest feeds can cheat with individual metrics, but not with FeedRank.

Individual metrics



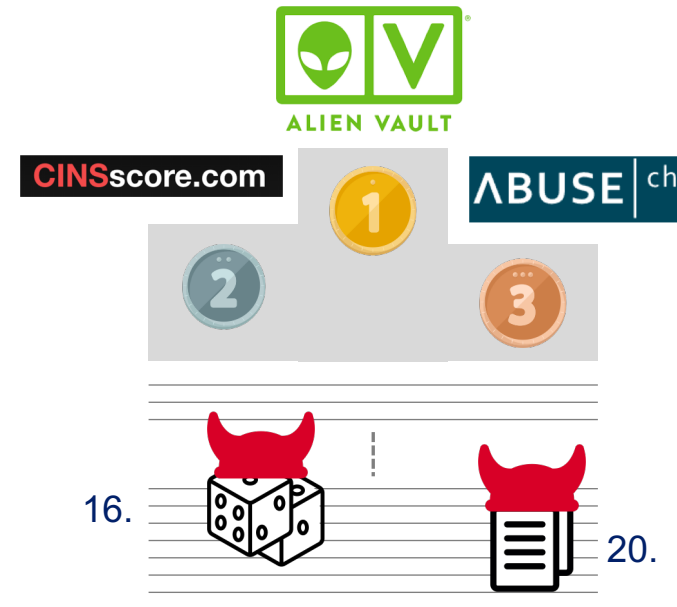
RandomFeed



CopyFeed



FeedRank



FeedRank

Evaluate cyber threat intelligence feeds in a way that

Correlation & Contribution analysis ■ Allows us to identify high quality feeds

Weights for correlation and contribution ■ Is customizable for different preferences of network defenders

Based solely on the contents of feeds ■ Does not require a ground truth

Well-known graph algorithms ■ Scales to the large ecosystem of feeds

Reputation-based PageRank algorithm ■ Is robust against dishonest feed providers

FeedRank

Evaluate cyber threat intelligence feeds in a way that

Correlation & Contribution analysis ■ Allows us to identify high quality feeds

Weights for correlation and contribution ■ Is customizable for different preferences of network defenders

Based solely on the contents of feeds ■ Does not require a ground truth

Well-known graph algorithms ■ Scales to the large ecosystem of feeds

Reputation-based PageRank algorithm ■ Is robust against dishonest feed providers

Questions?