Forward-Looking Statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

splunk> .conf21

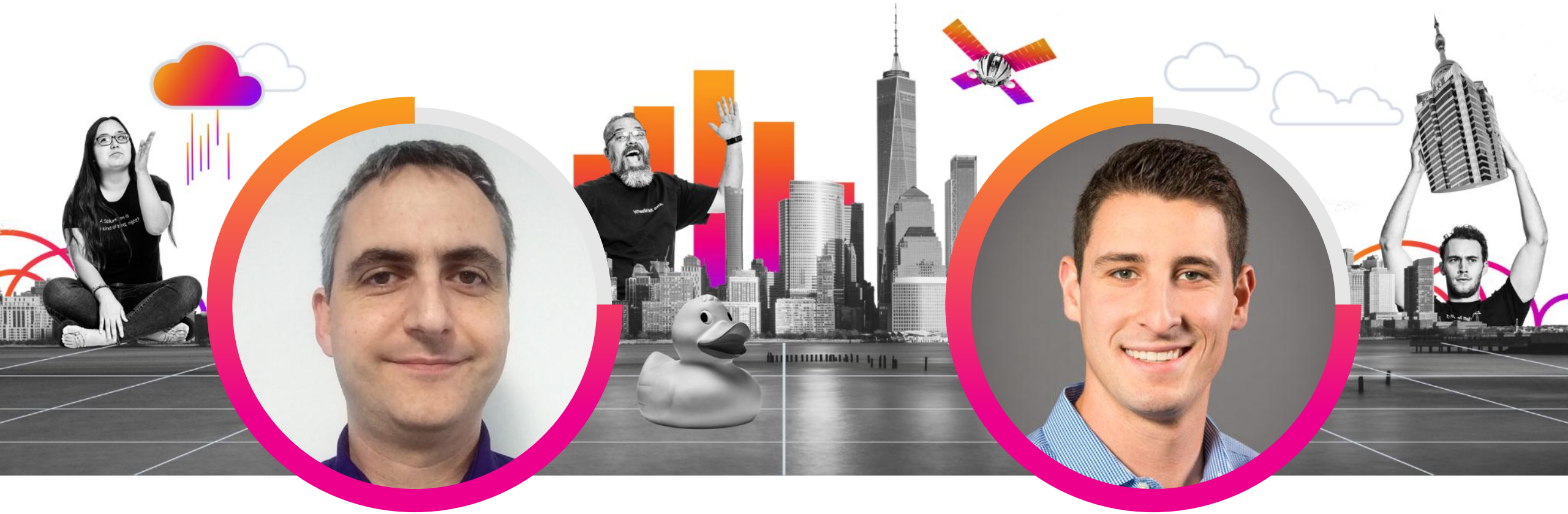
Advanced Scheduling with Splunk to Help Ensure Your Searches Run, Succeed and Cover All Data

PLA1372B

Andrew Smith
Manager Cybersecurity Analytics | Pfizer

Maksim Dubyk
Manager Intrusion Detection & Analysis | Pfizer

splunk> .conf21



Andrew Smith

Manager Cybersecurity Analytics | Pfizer

Maksim Dubyk

Manager Intrusion Detection & Analysis | Pfizer

splunk> .conf21

Agenda

1) Alerting Challenges

2) Ineffective Solutions

3) Our Solution: Stateful earliest index time

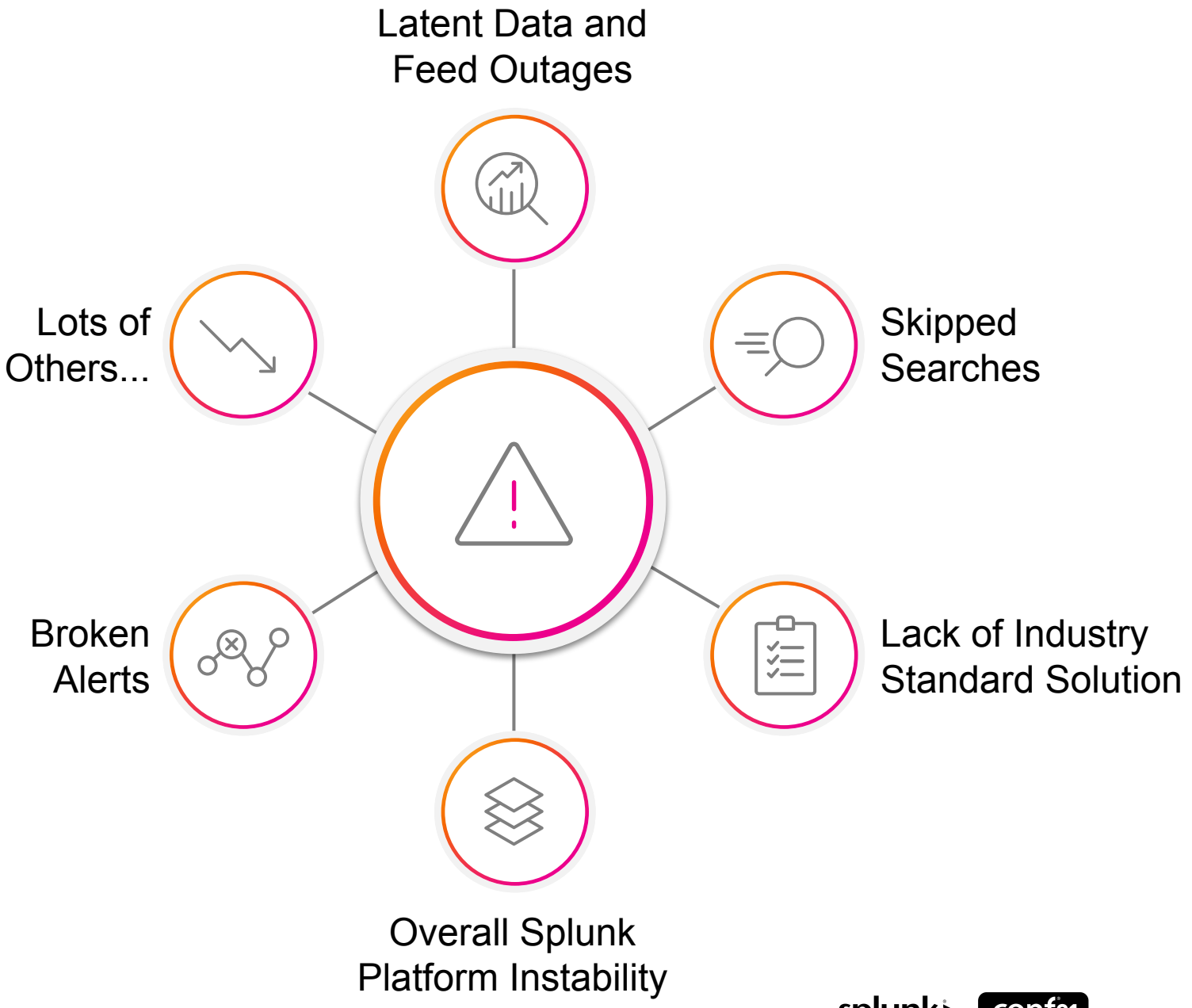
4) Complex Use Cases with Apache Airflow

5) “So How Do I Get Started?”

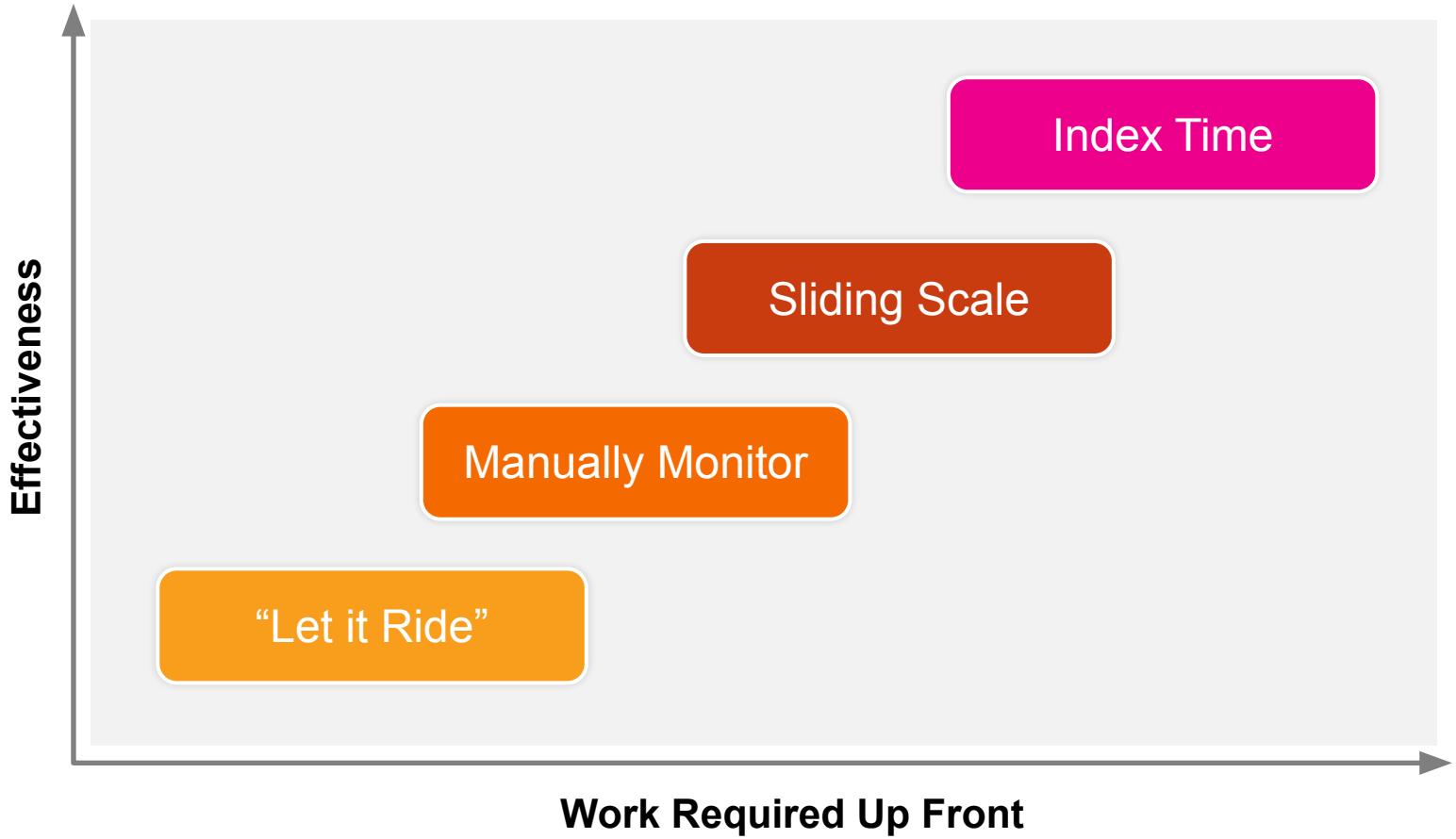
Disclaimer: this presentation, and any related discussions are solely the views, opinions and experiences of the presenter(s) and should not be presumed to reflect the opinion or the official position of Pfizer Inc. Examples and views provided herein, including strategies, goals, targets and indicators, are for illustrative purposes only and should not be regarded as representative of Pfizer Inc. or its portfolio.

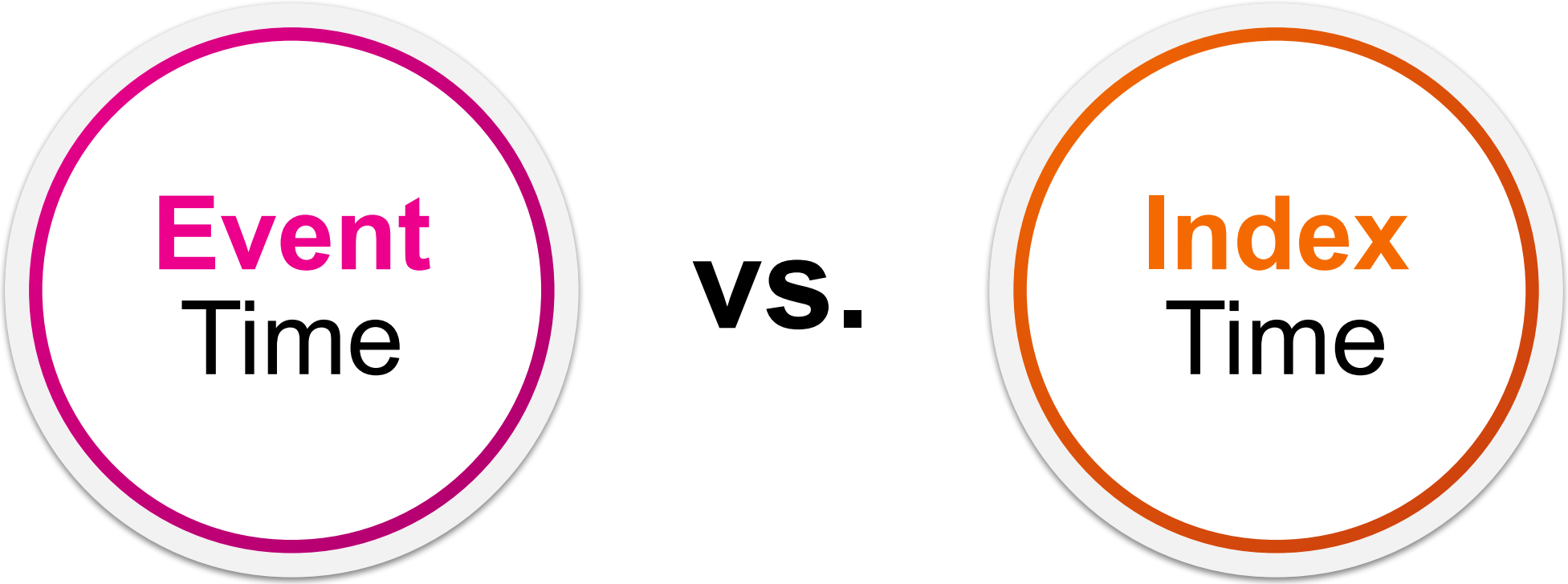
To the extent that this presentation outlines a general technology direction, Pfizer Inc. has no obligation to pursue any such approach or to develop or use any functionality mentioned herein. Any suggested technology strategy or possible future developments are subject to change, at Pfizer's sole discretion and without notice.

Splunk Alerting Challenges



How do Most People Address These Issues?





The Progression of How to Query

```
index=firewall badness_detected=true
| eval a="bcde"
| ...
```

Last 60 minutes

```
index=firewall badness_detected=true earliest=-1h@h latest=-0h@h
| eval a="bcde"
| ...
```

```
index=firewall badness_detected=true _index_earliest=-1h@h _index_latest=-0h@h
| eval a="bcde"
| ...
```

```
index=firewall badness_detected=true `autotimeframe("The Alert Name")`
| eval a="bcde"
| ...
```

Our Solution

- Uses index time
- Decouple execution time from search time
- KV store records "Last Ran"
- Macro reads and updates "Last Ran"
- Safeguards:
  - Limits maximum search
  - Includes a rolling overlap window
- Manual override for manual re-runs

KV Store

Alert Name	Last Ran
The Alert Name	2021-09-01:10:15:00

Macro

```
[| makeresults
    | fields - _time
    | eval query_name_hash = md5("$query_name$")
    | lookup lastrun _key AS query_name_hash
    | eval last_time = max(coalesce(last_time, relative_time(now(), "-$default_start_lookback$") - 1), relative_time(now(), "-$longest_lookback$"))
    | eval search_to = min(relative_time(now(), "-$realtime_lag$"), relative_time(last_time, "+$longest_query$"))
    | eval search_from = relative_time(last_time, "-$overlap$")
    | eval search = "_index_earliest=".search_from." _index_latest=".search_to." earliest=$event_time_earliest$ latest=$event_time_latest$"
    | appendpipe
        [| eval _key = query_name_hash
        | eval last_time = search_to
        | fields + last_time, _key
        | outputlookup append=t lastrun
        | where 1=2 ]
    | fields + search ]
```

Alert

```
index=firewall badness_detected=true `autotimeframe("The Alert Name")`
| eval a="bcde"
| ...
```

A Look at the Macro

```
[| makeresults
    | fields - _time
    | eval query_name_hash = md5("$query_name$")
    | lookup lastrun _key AS query_name_hash
    | eval last_time = max(coalesce(last_time, relative_time(now(), "-$default_start_lookback$") - 1), relative_time(now(), "-$longest_lookback$"))
    | eval search_to = min(relative_time(now(), "-$realtime_lag$"), relative_time(last_time, "+$longest_query$"))
    | eval search_from = relative_time(last_time, "-$overlap$")
    | eval search = " index earliest=".search_from." index latest=".search_to." earliest=$event_time_earliest$ latest=$event_time_latest$"
    | appendpipe
        [| eval _key = query_name_hash
        | eval last_time = search_to
        | fields + last_time, _key
        | outputlookup append=t lastrun
        | where 1=2 ]
    | fields + search ]
```

Find the last time the named query ran until from the KVStore

Update the KVStore ready for the next execution

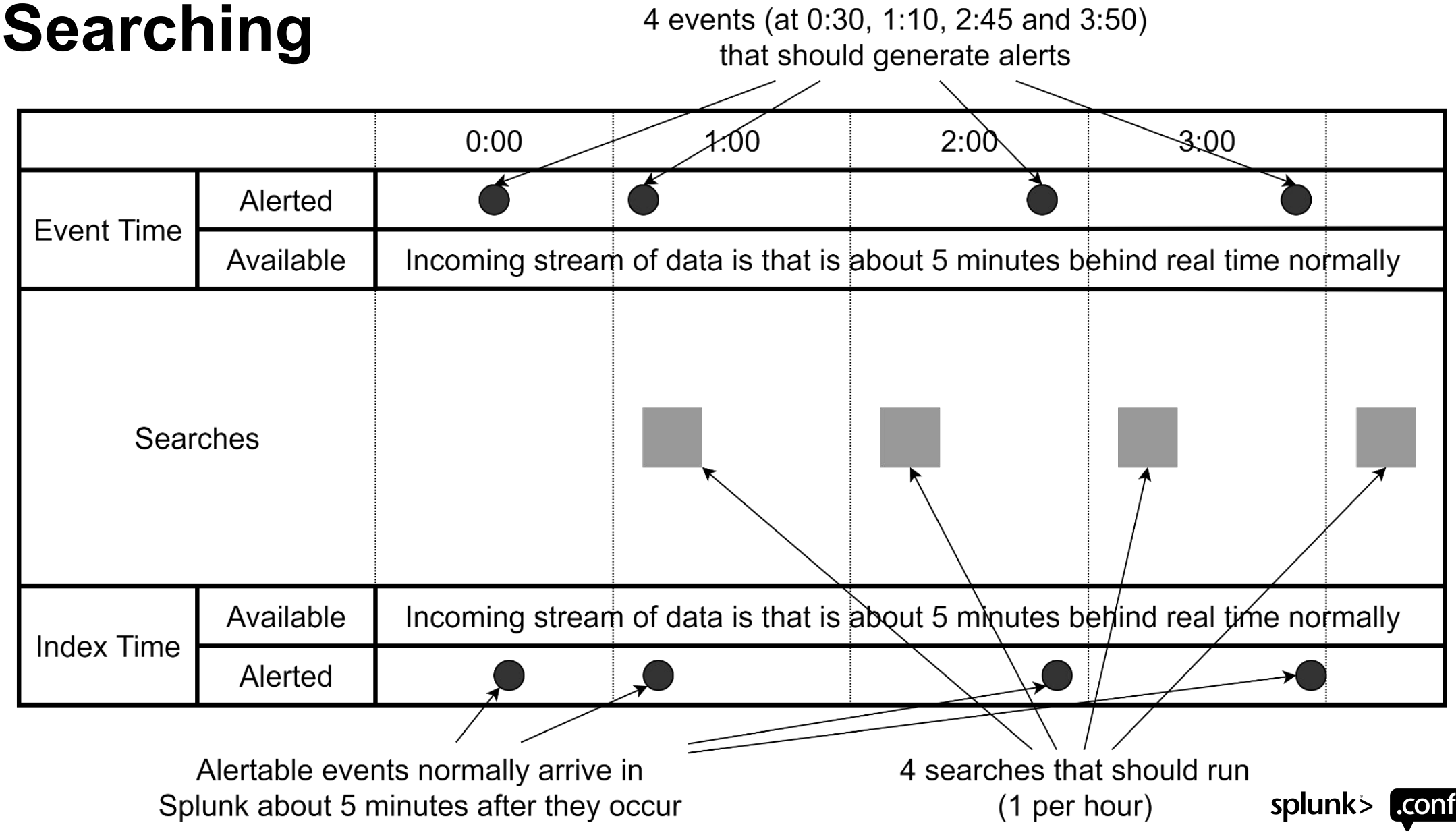
Generate the timeframe to apply to the search

Challenges Addressed

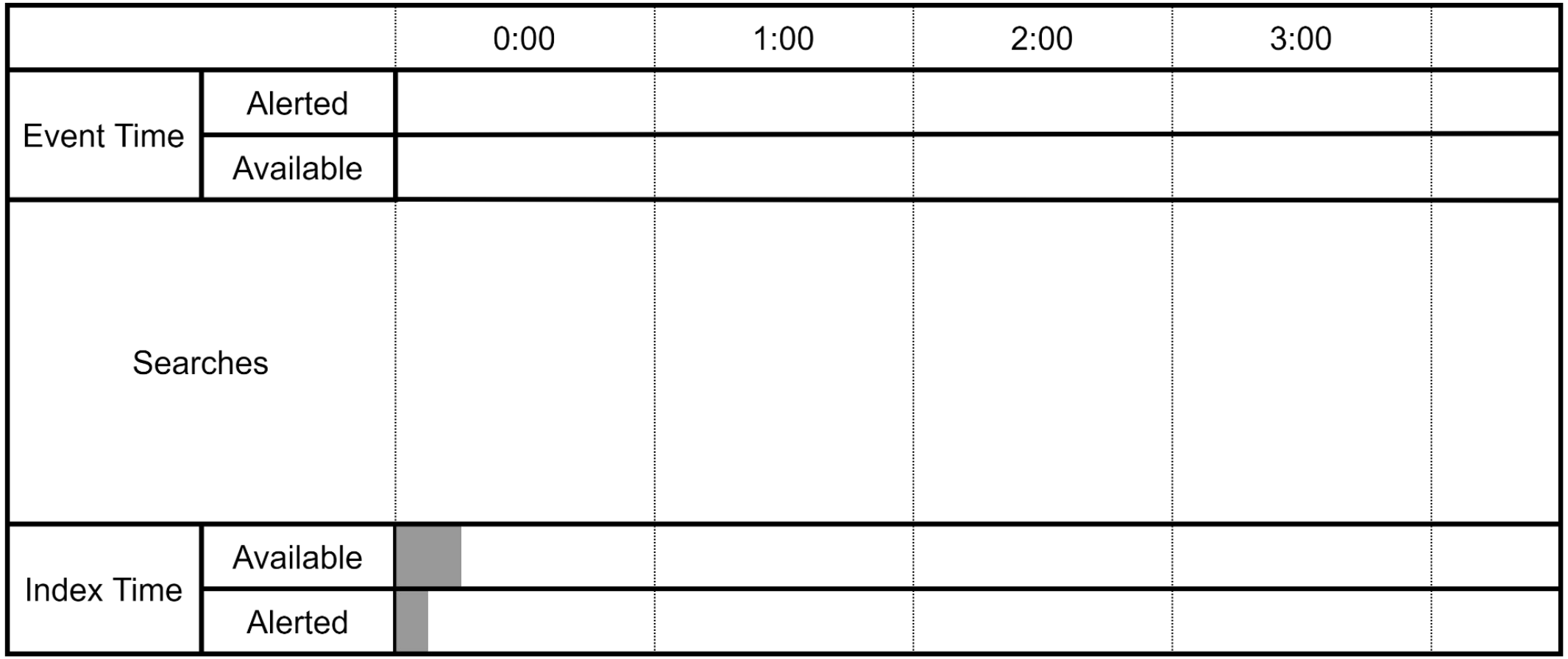
- Latent data that is an hour + behind
- Feed outage stops for 5 hours
- Search head down / skipped searches
- Broken search due to user SPL error

Scenario: Normal Conditions
Time Source: Event Time Searching

Searching



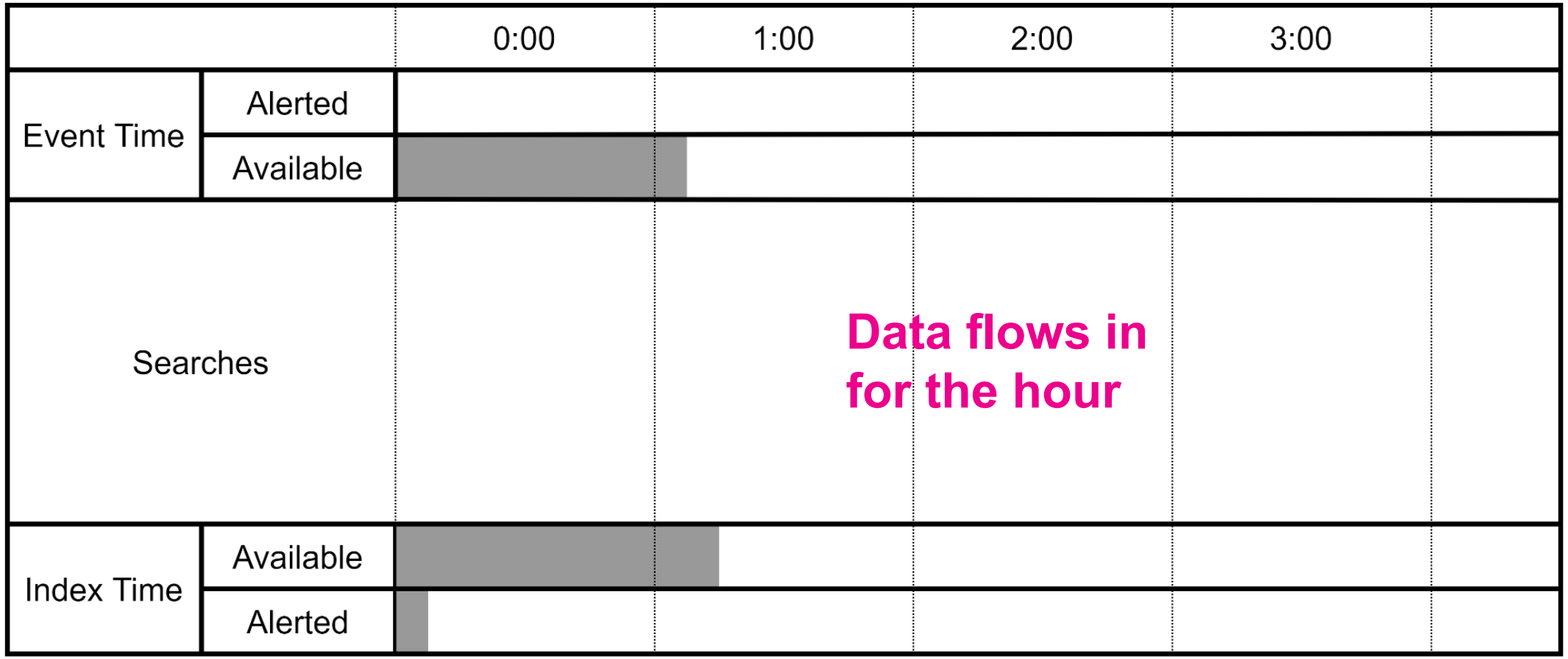
Normal Conditions | Event Time Searching



Time: 00:10

Alerts Raised: 0 of 0

Normal Conditions | Event Time Searching



Time: 01:10

Alerts Raised: 0 of 0

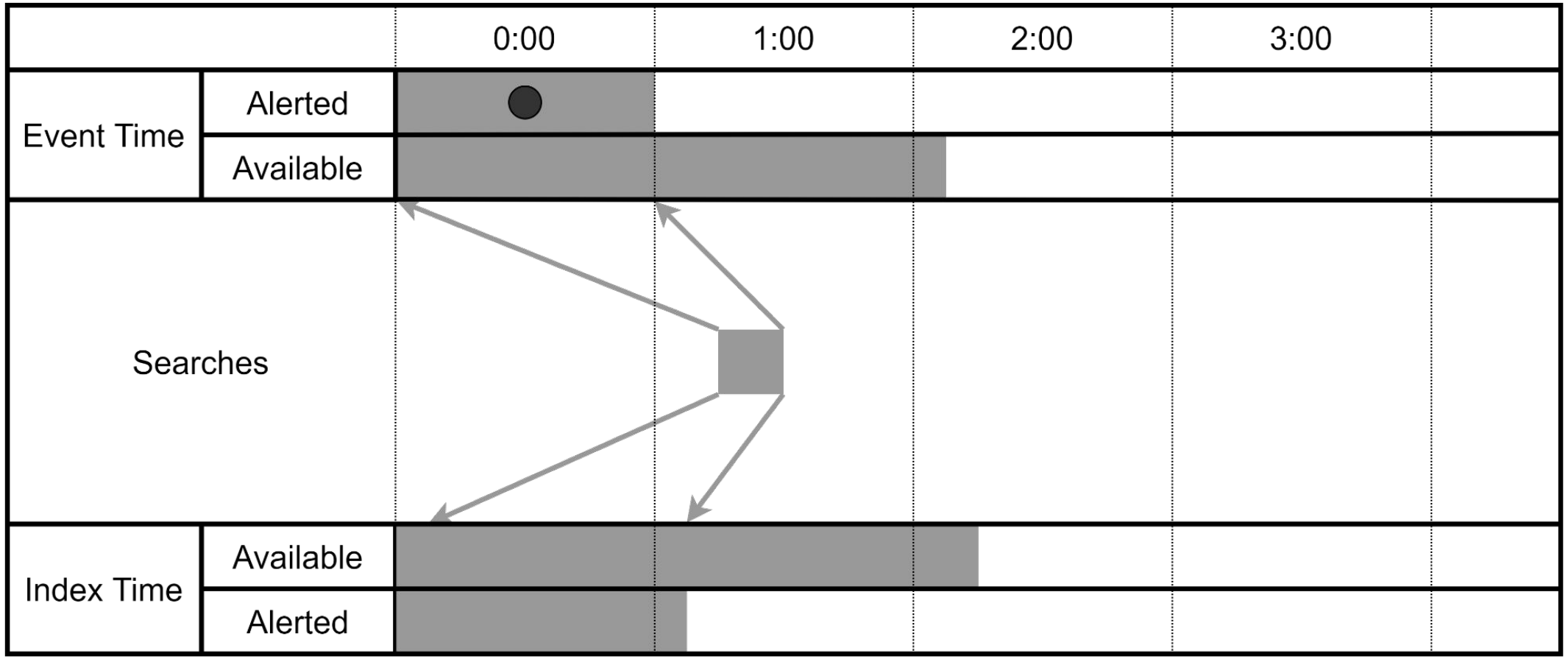
splunk> .conf21

Normal Conditions | Event Time Searching

Time: 00:10

Alerts Raised: 1 of 1

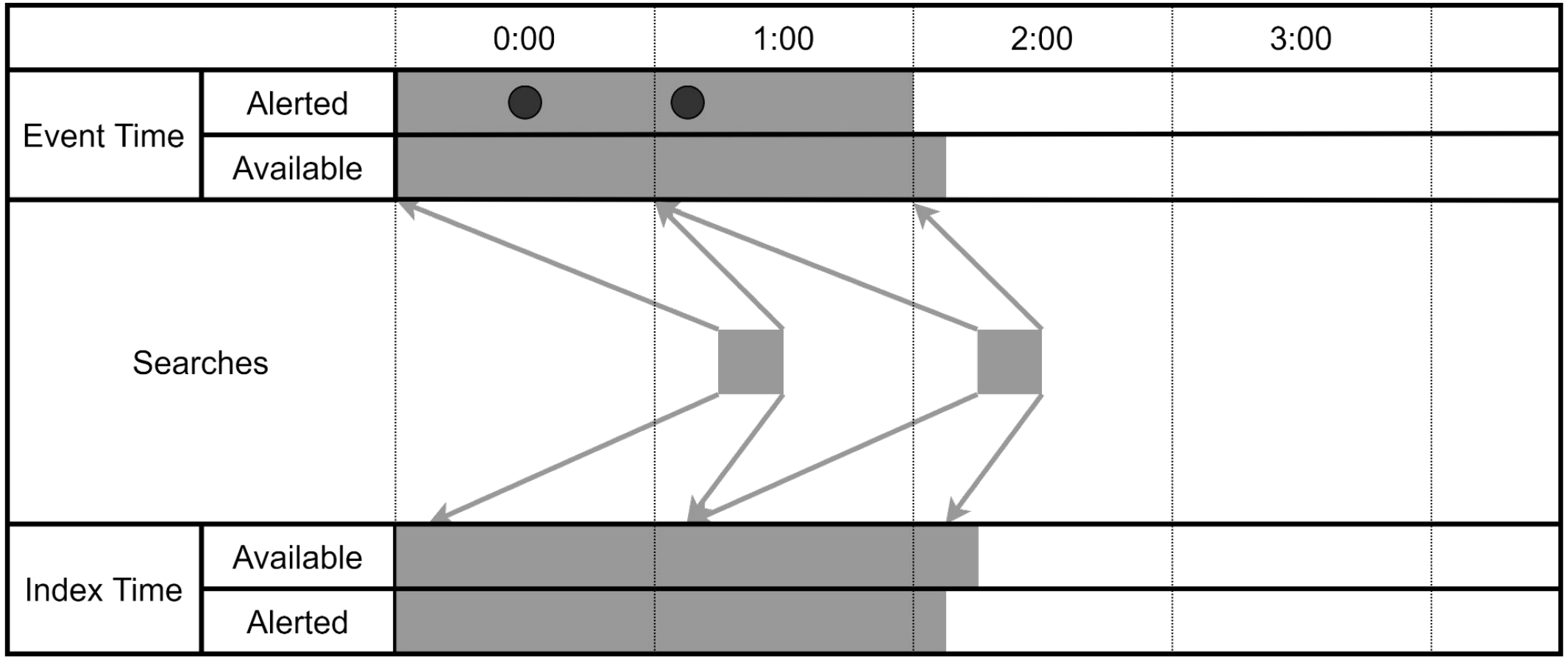
Normal Conditions | Event Time Searching



Time: 02:10

Alerts Raised: 1 of 1

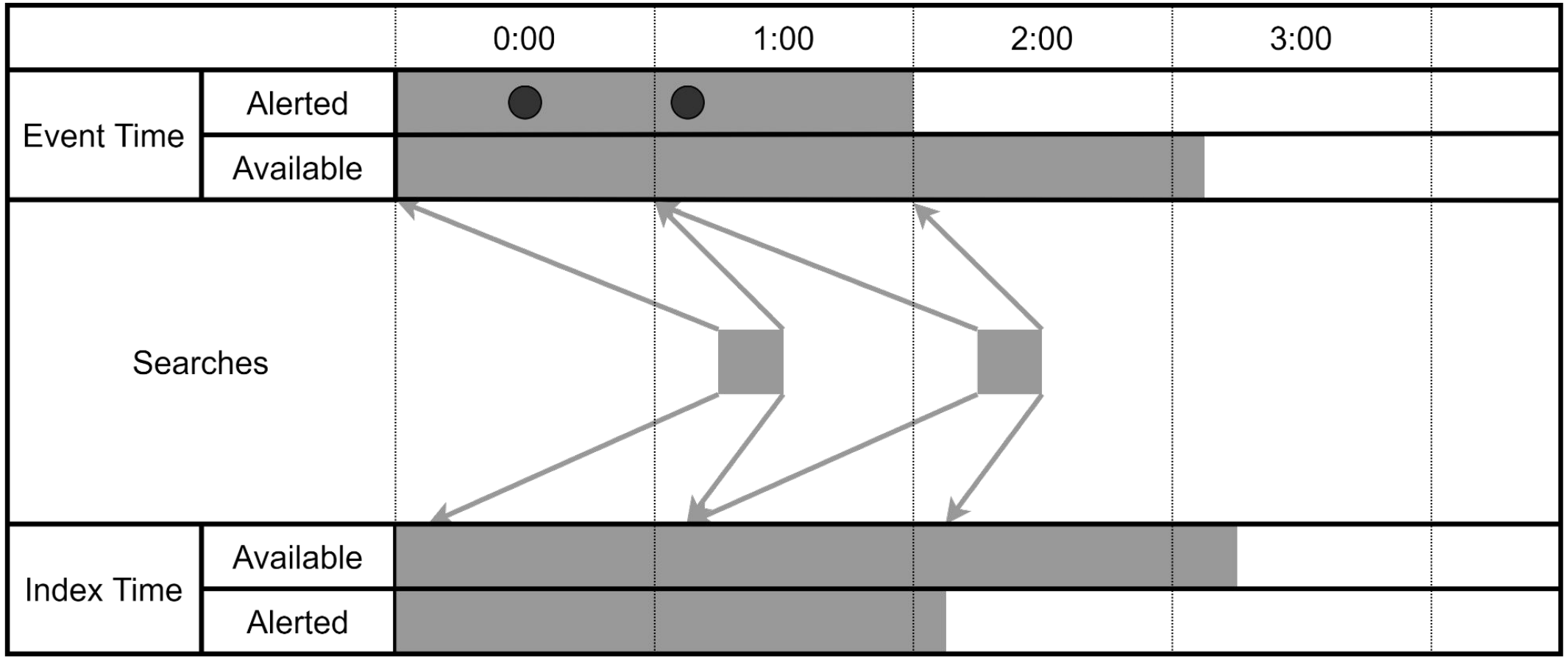
Normal Conditions | Event Time Searching



Time: 02:10

Alerts Raised: 2 of 2

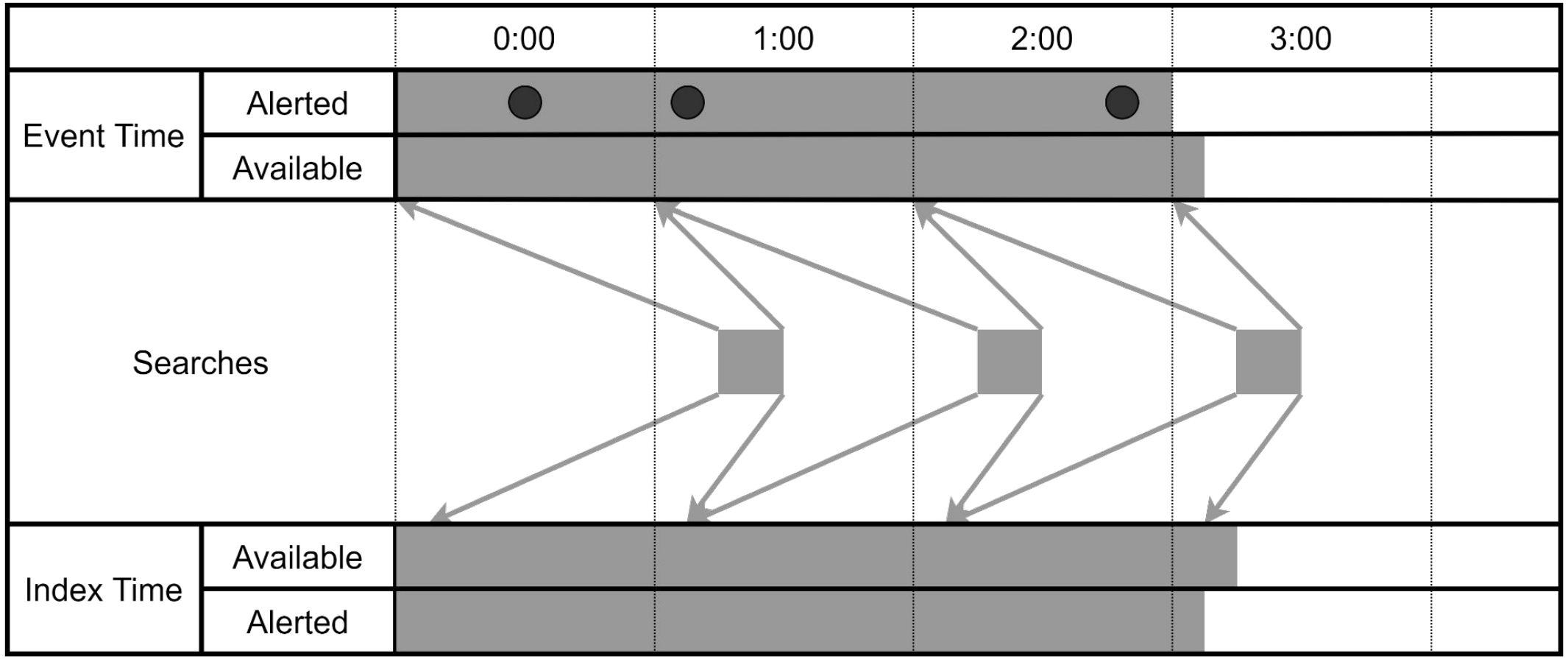
Normal Conditions | Event Time Searching



Time: 03:10

Alerts Raised: 2 of 2

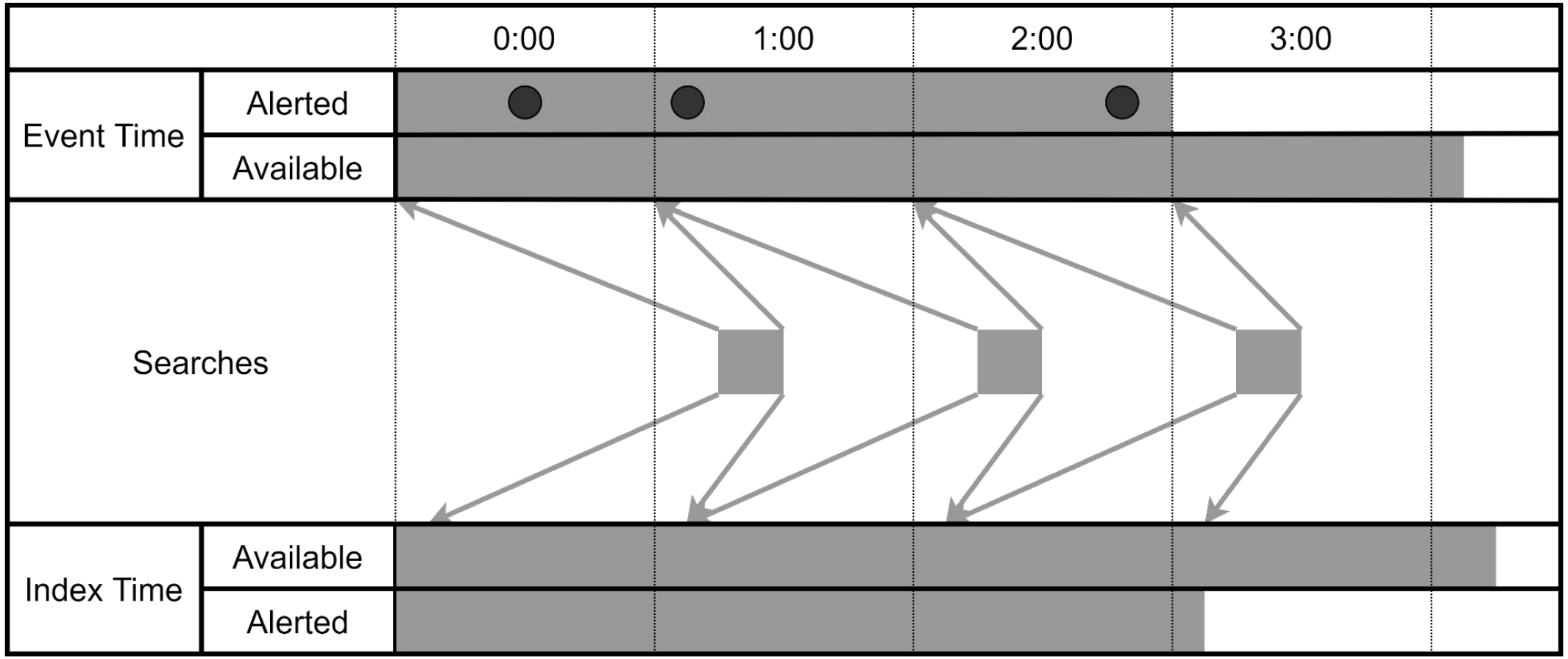
Normal Conditions | Event Time Searching



Time: 03:10

Alerts Raised: 3 of 3

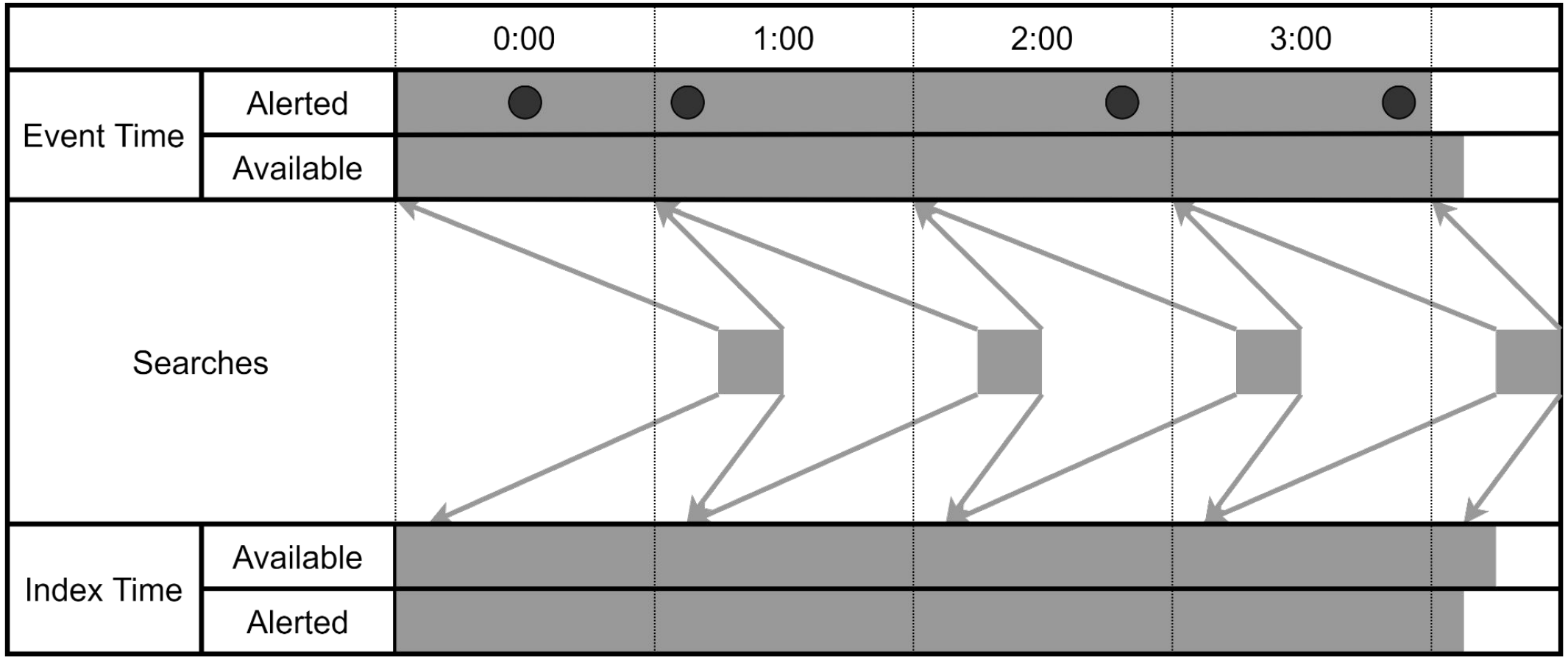
Normal Conditions | Event Time Searching



Time: 04:10

Alerts Raised: 3 of 3

Normal Conditions | Event Time Searching

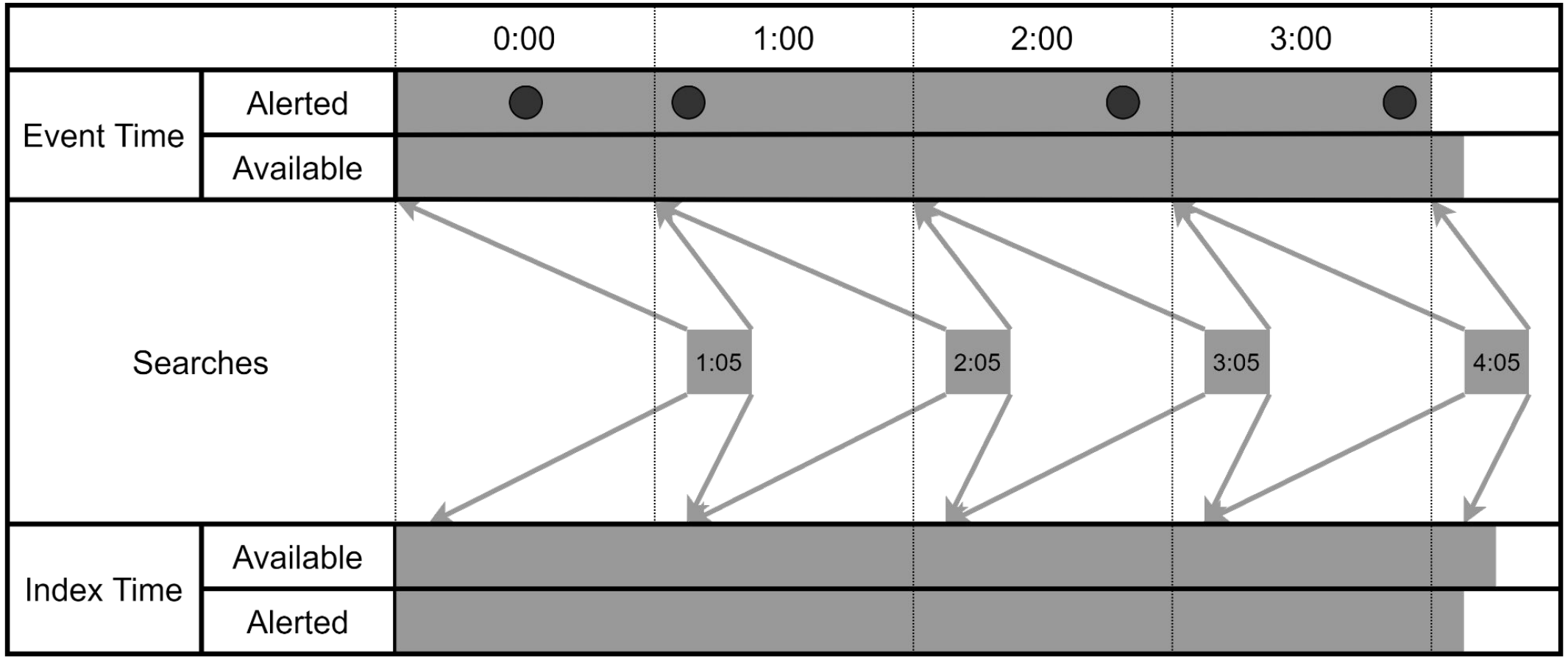


Time: 04:10

Alerts Raised: 4 of 4

Scenario: Normal Conditions
Time Source: Index Time Searching

Normal Conditions | Index Time Searching



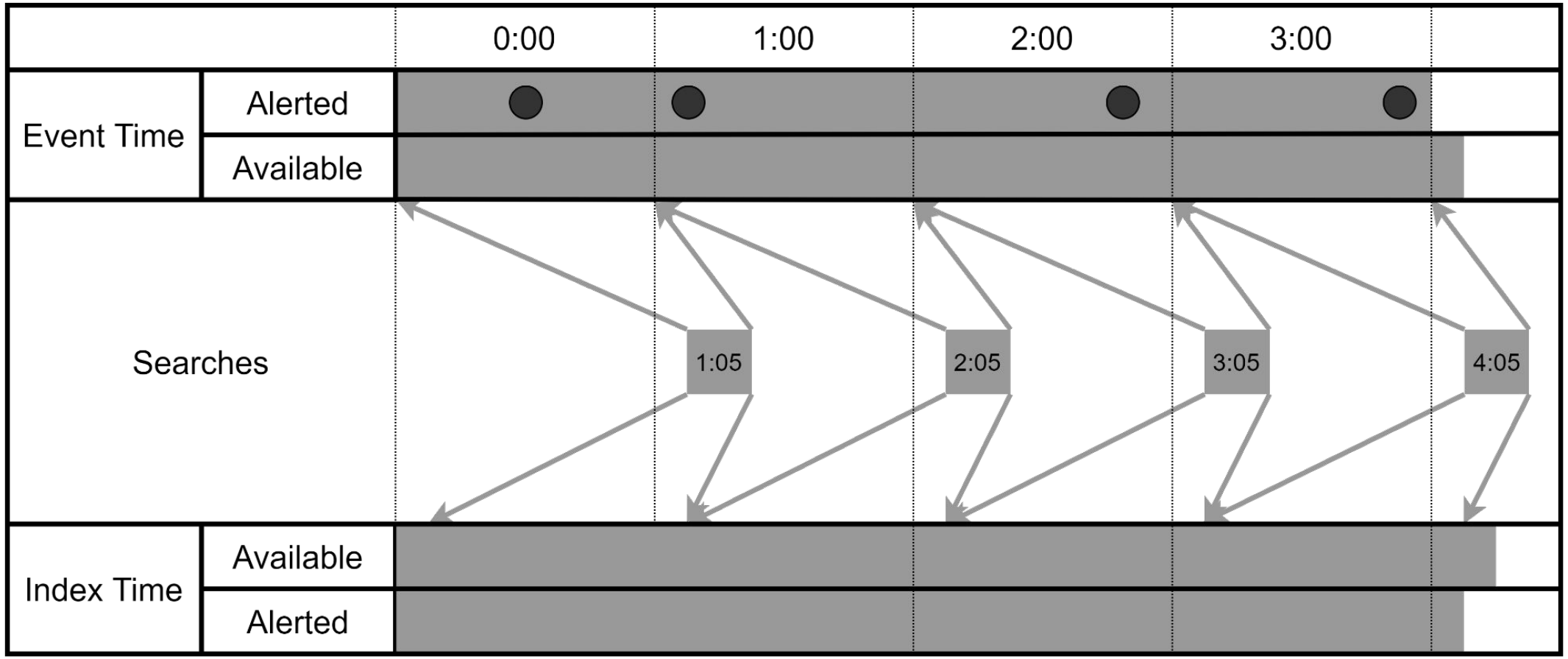
Time: 04:05

Alerts Raised: 4 of 4

splunk> .conf21

Scenario: Normal Conditions
Time Source: Macro Method Searching

Normal Conditions | Macro Method Searching



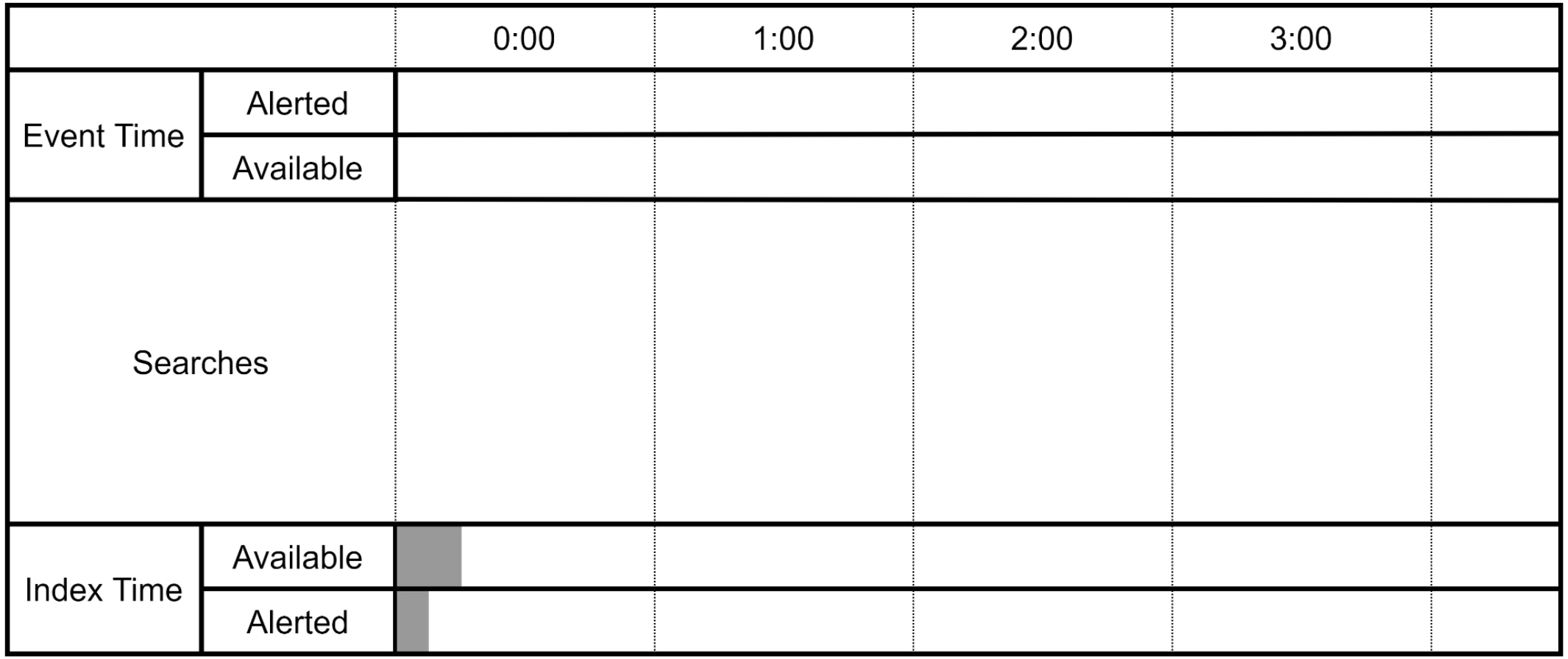
Time: 04:05

Alerts Raised: 4 of 4

splunk> .conf21

Scenario: Latent Data
Time Source: Event Time Searching

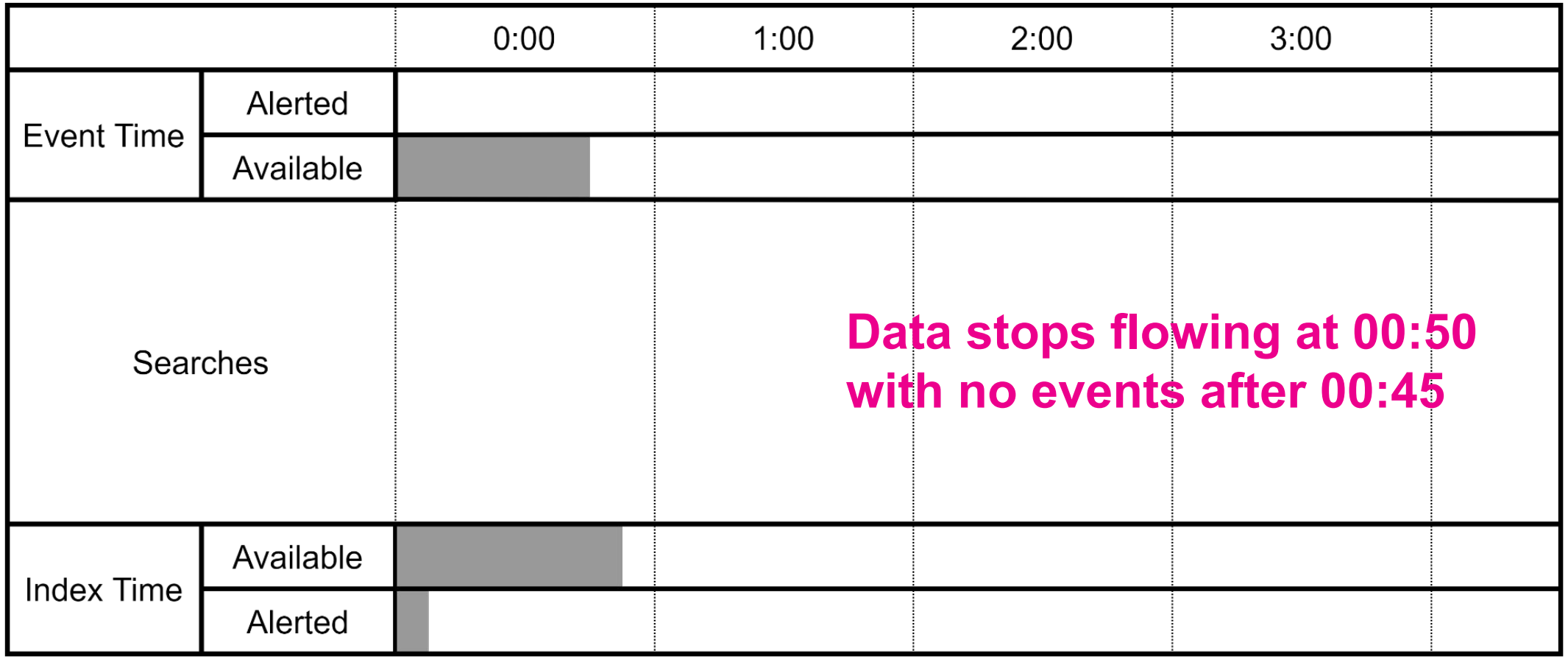
Latent Data | Event Time Searching



Time: 00:10

Alerts Raised: 0 of 0

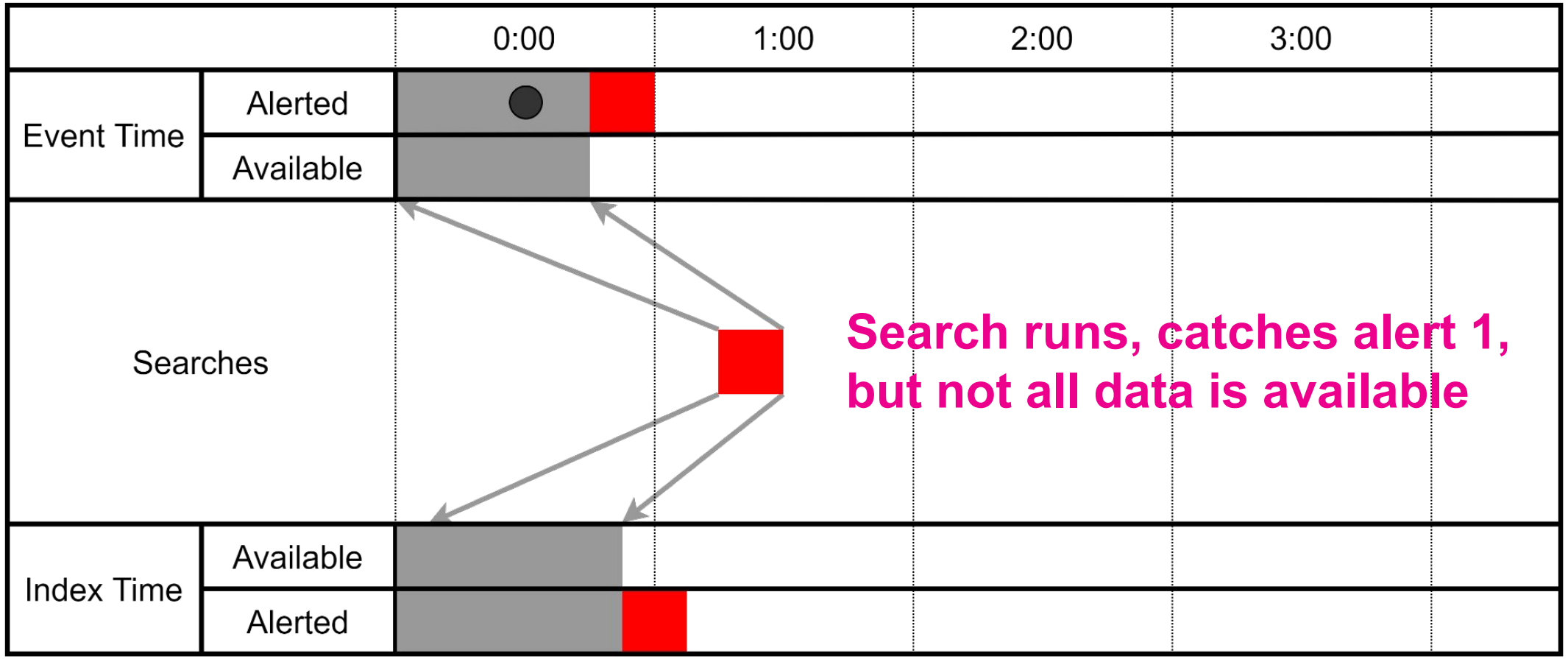
Latent Data | Event Time Searching



Time: 01:10

Alerts Raised: 0 of 0

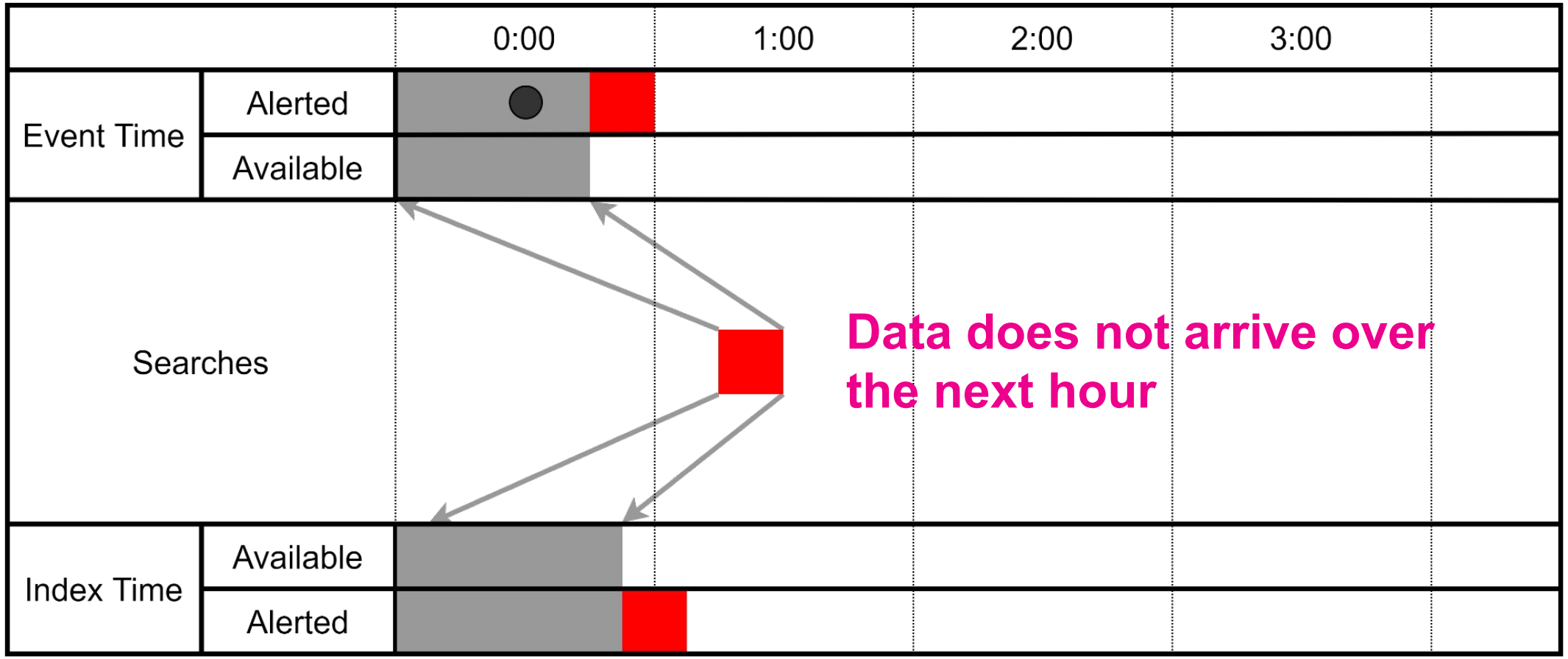
Latent Data | Event Time Searching



Time: 01:10

Alerts Raised: 1 of 1

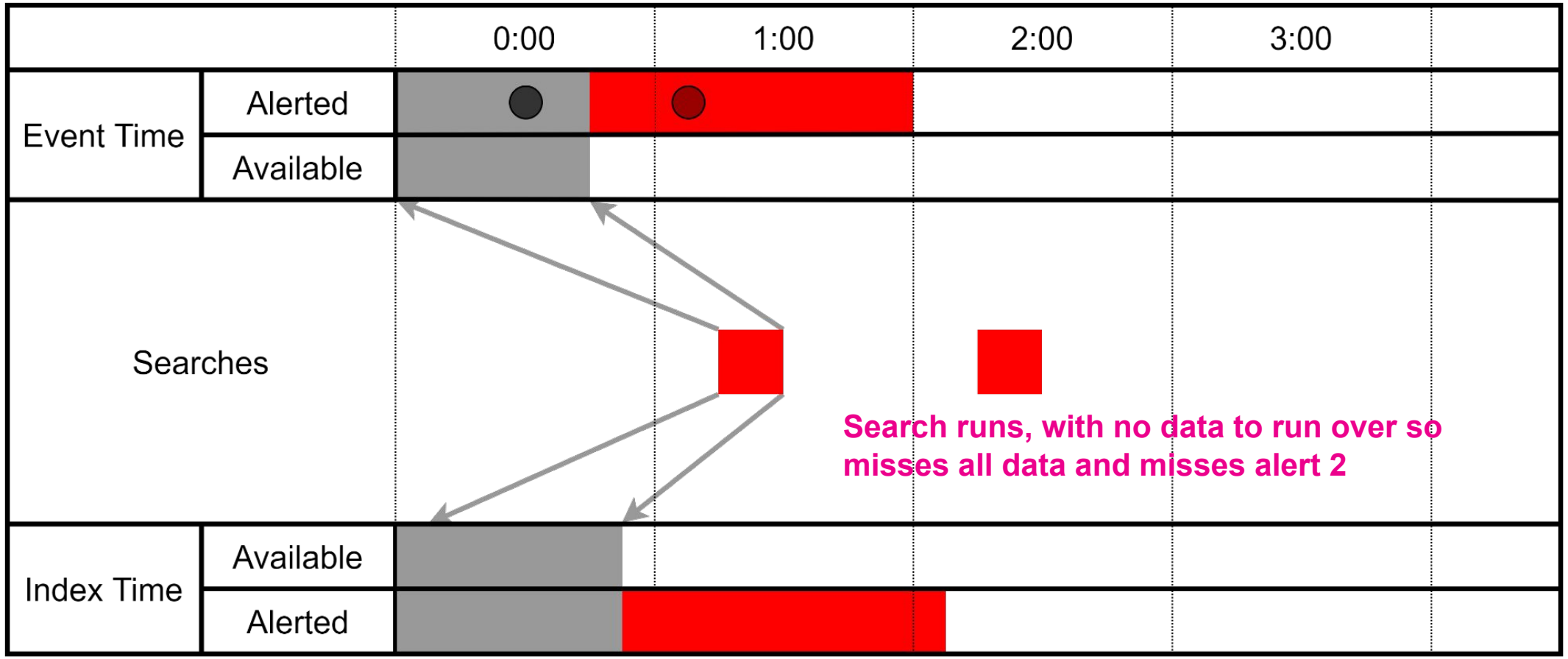
Latent Data | Event Time Searching



Time: 02:10

Alerts Raised: 1 of 1

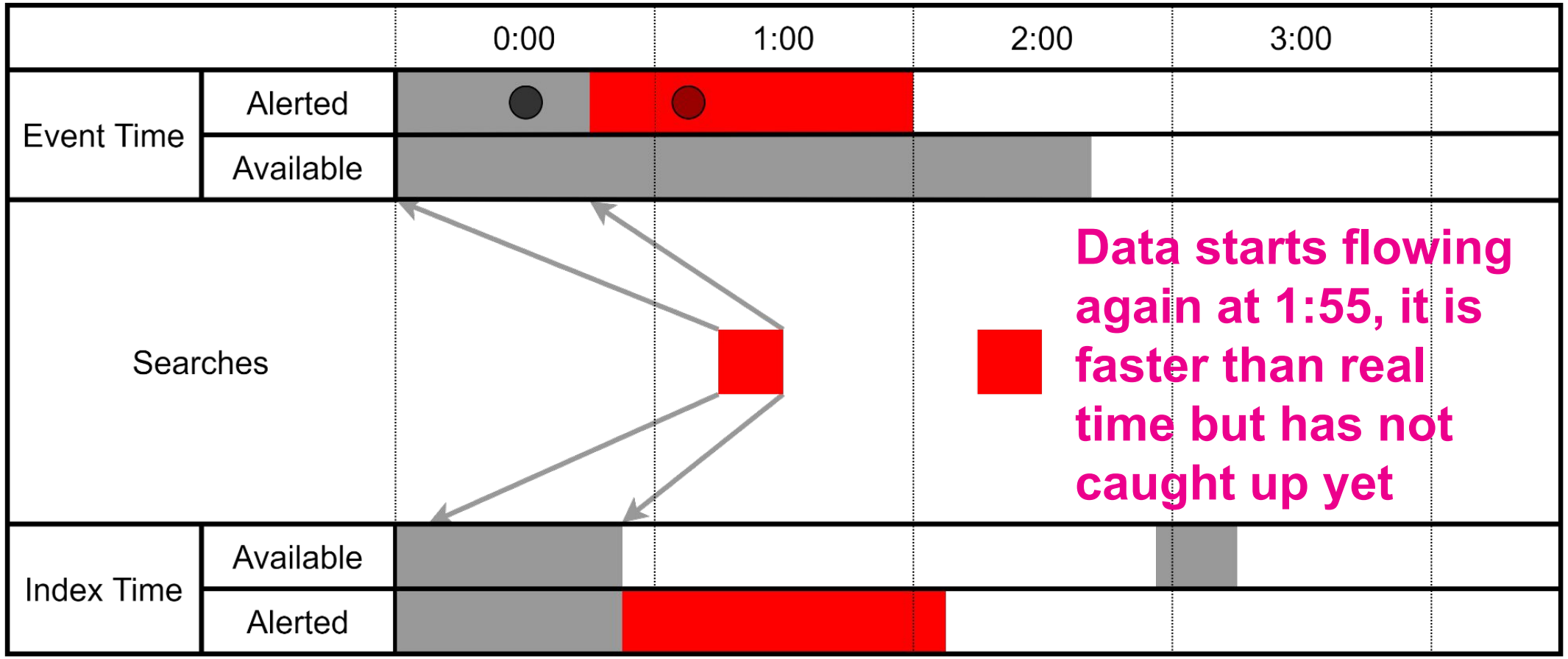
Latent Data | Event Time Searching



Time: 02:10

Alerts Raised: 1 of 2

Latent Data | Event Time Searching

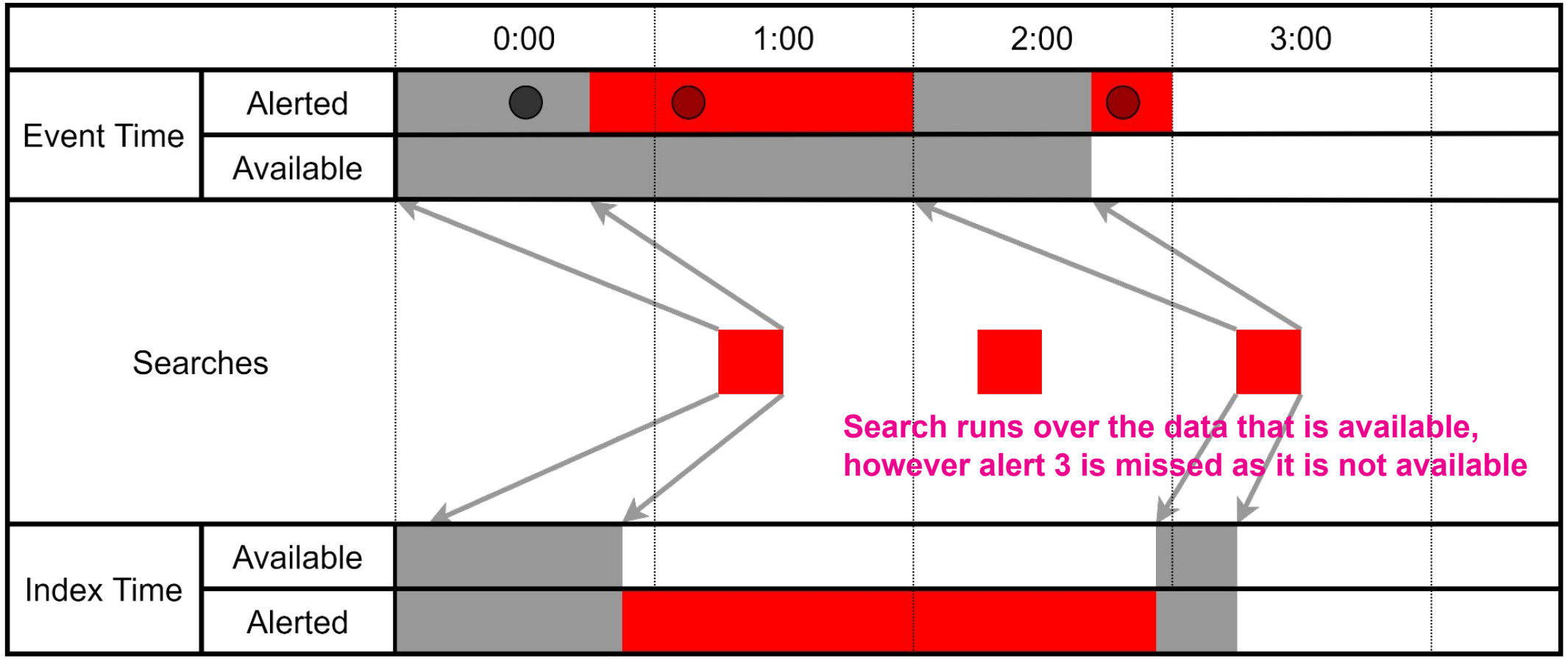


Time: 03:10

Alerts Raised: 1 of 2

splunk> .conf21

Latent Data | Event Time Searching

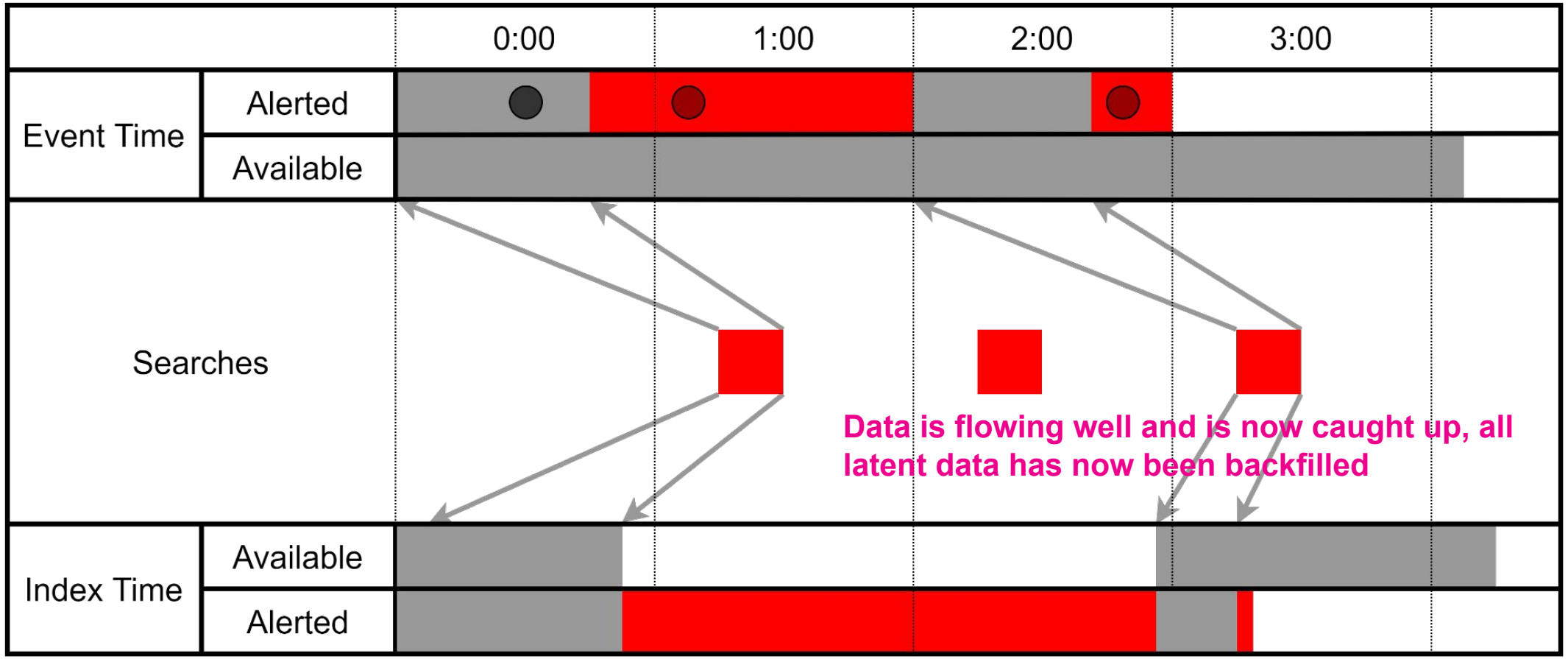


Time: 03:10

Alerts Raised: 1 of 3

splunk> .conf21

Latent Data | Event Time Searching

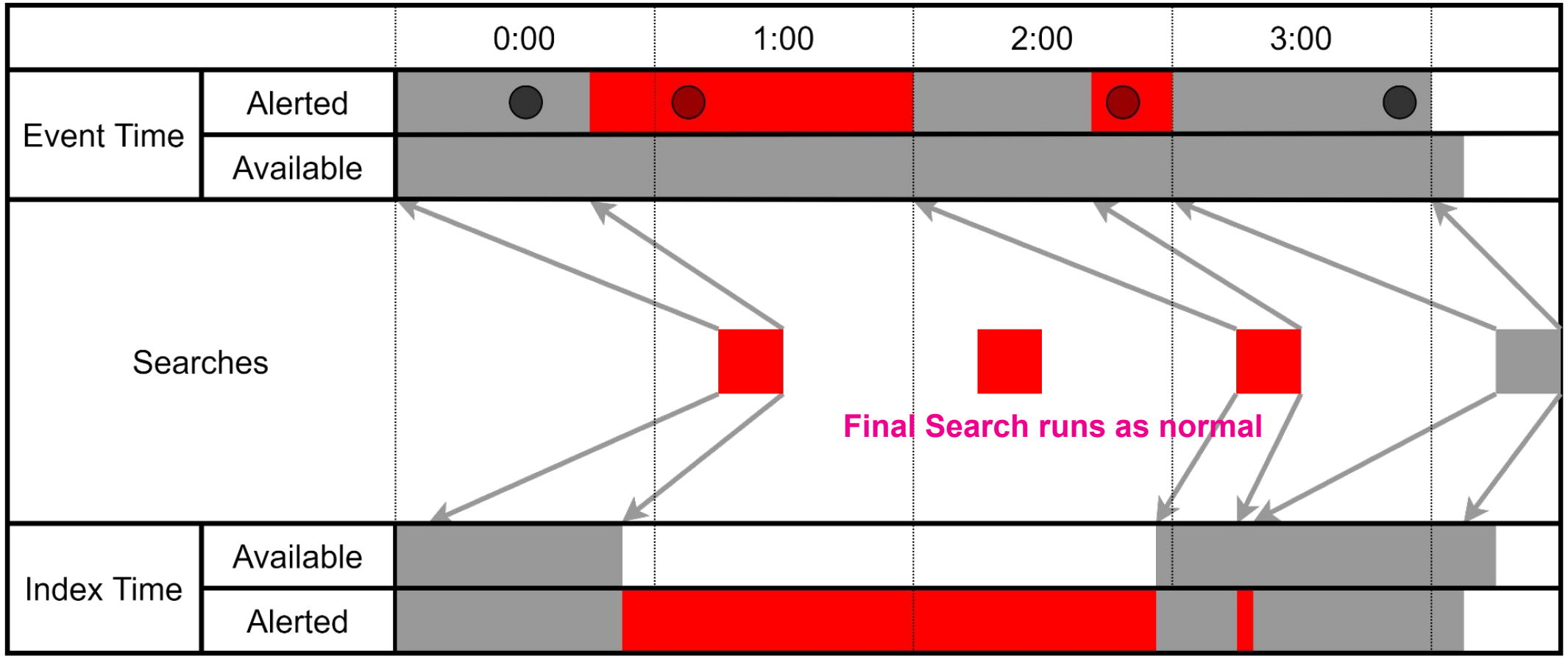


Time: 04:10

Alerts Raised: 1 of 3

splunk> .conf21

Latent Data | Event Time Searching

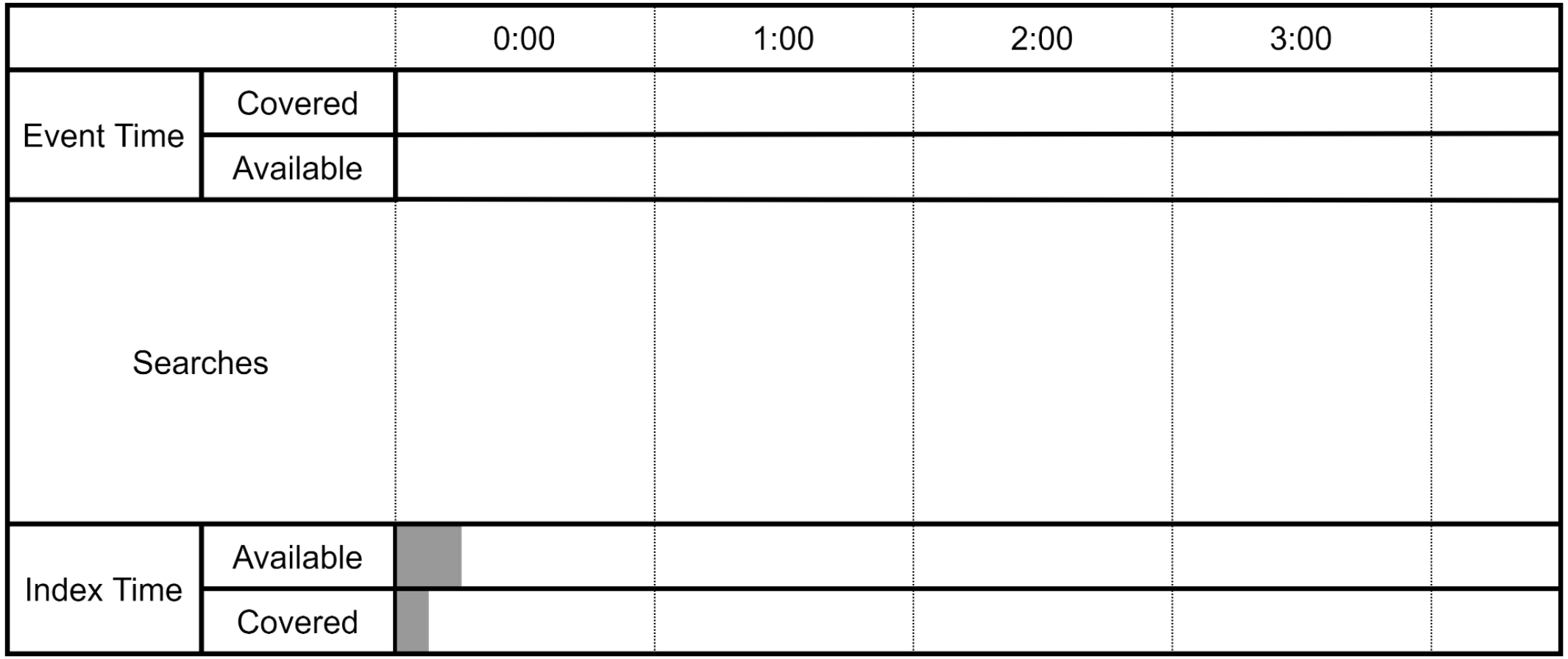


Time: 04:10

Alerts Raised: 2 of 4

Scenario: Latent Data
Time Source: Index Time Searching

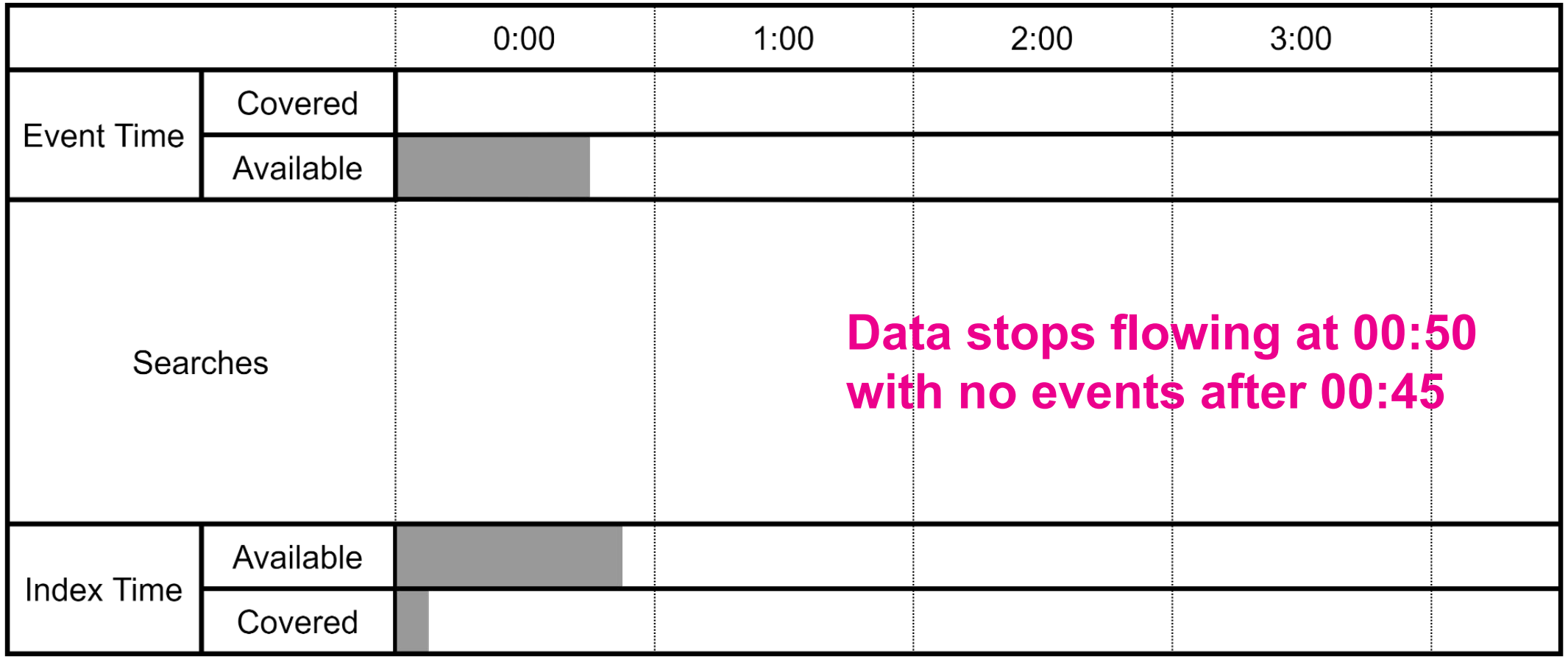
Latent Data | Index Time / Macro Method



Time: 00:10

Alerts Raised: 0 of 0

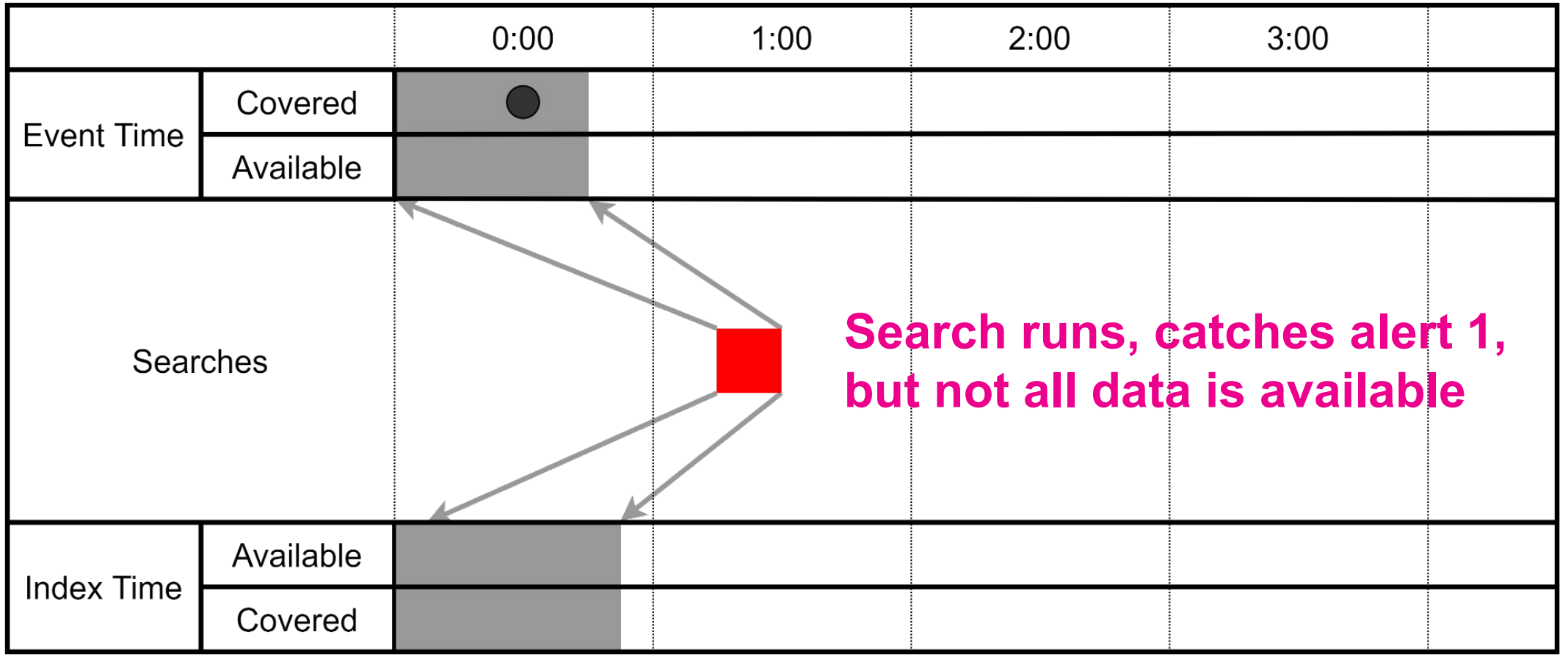
Latent Data | Index Time / Macro Method



Time: 01:10

Alerts Raised: 0 of 0

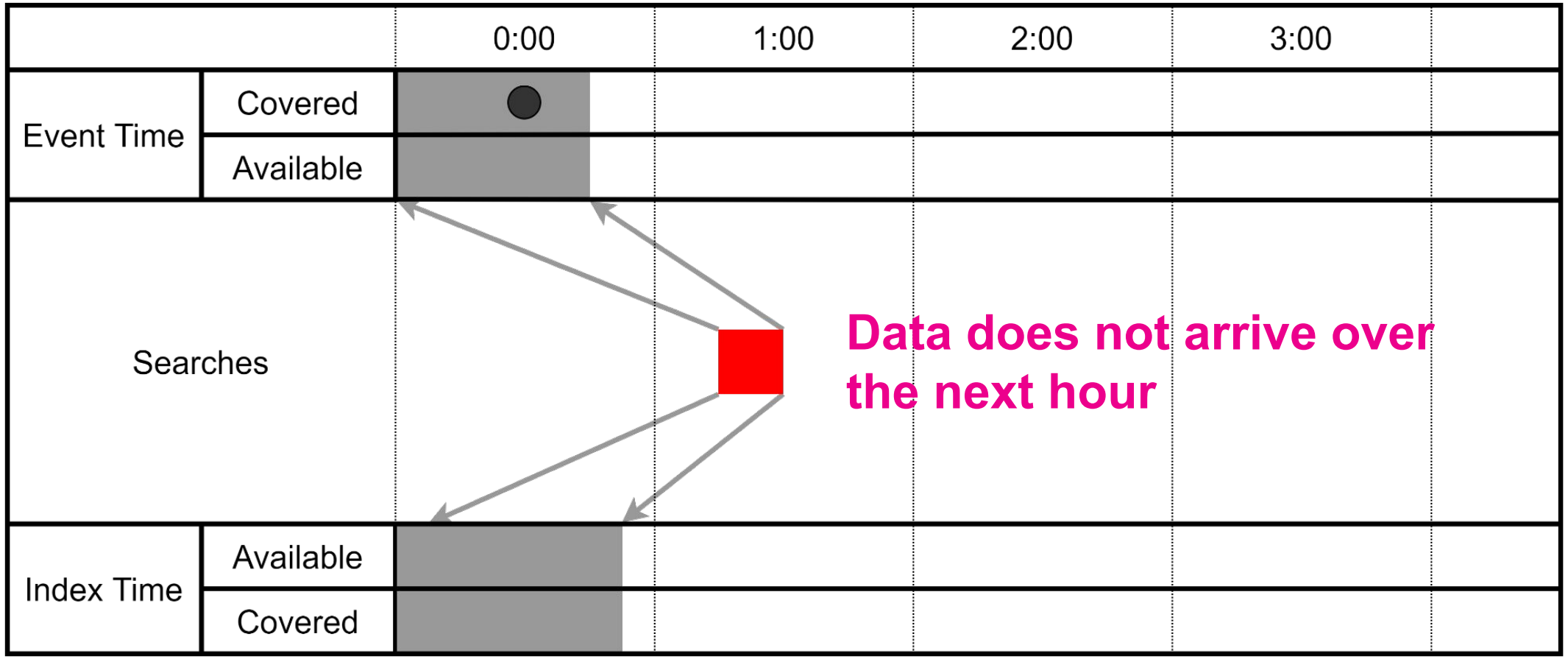
Latent Data | Index Time / Macro Method



Time: 01:10

Alerts Raised: 1 of 1

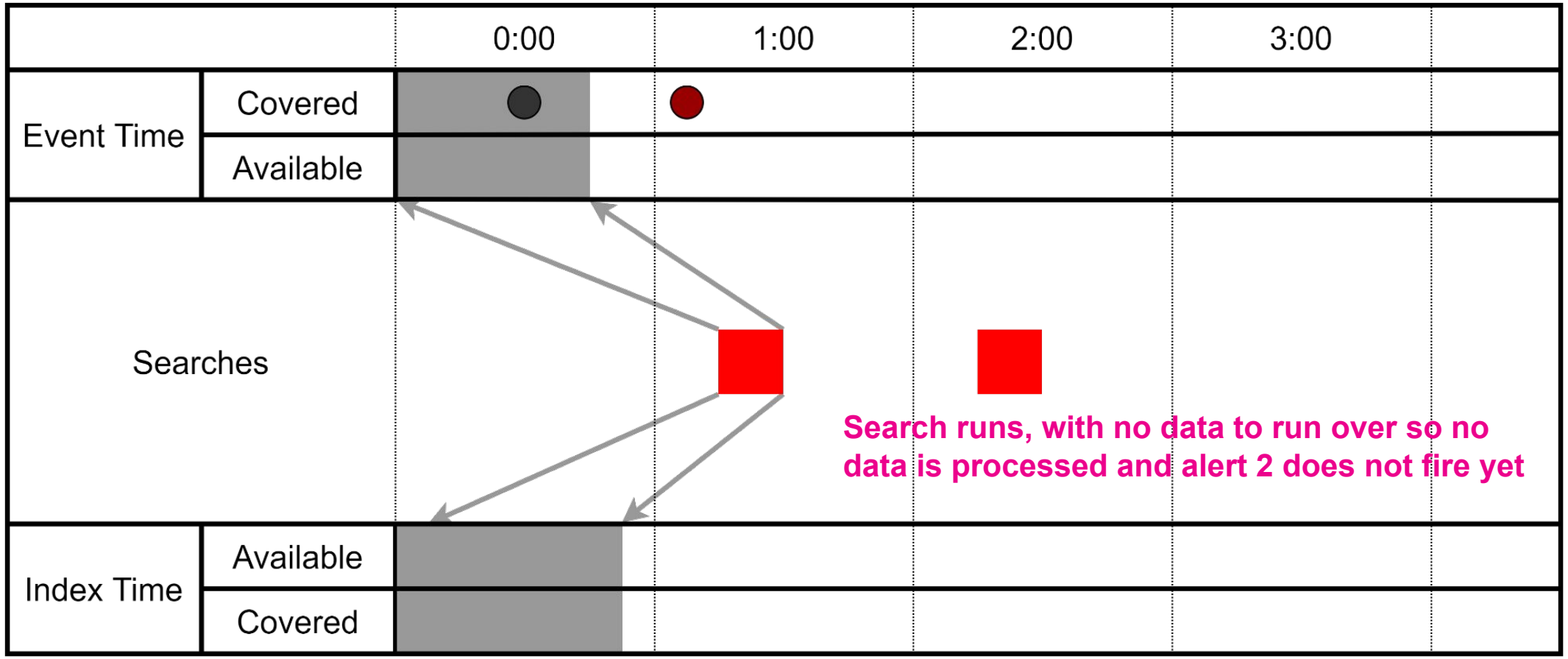
Latent Data | Index Time / Macro Method



Time: 02:10

Alerts Raised: 1 of 1

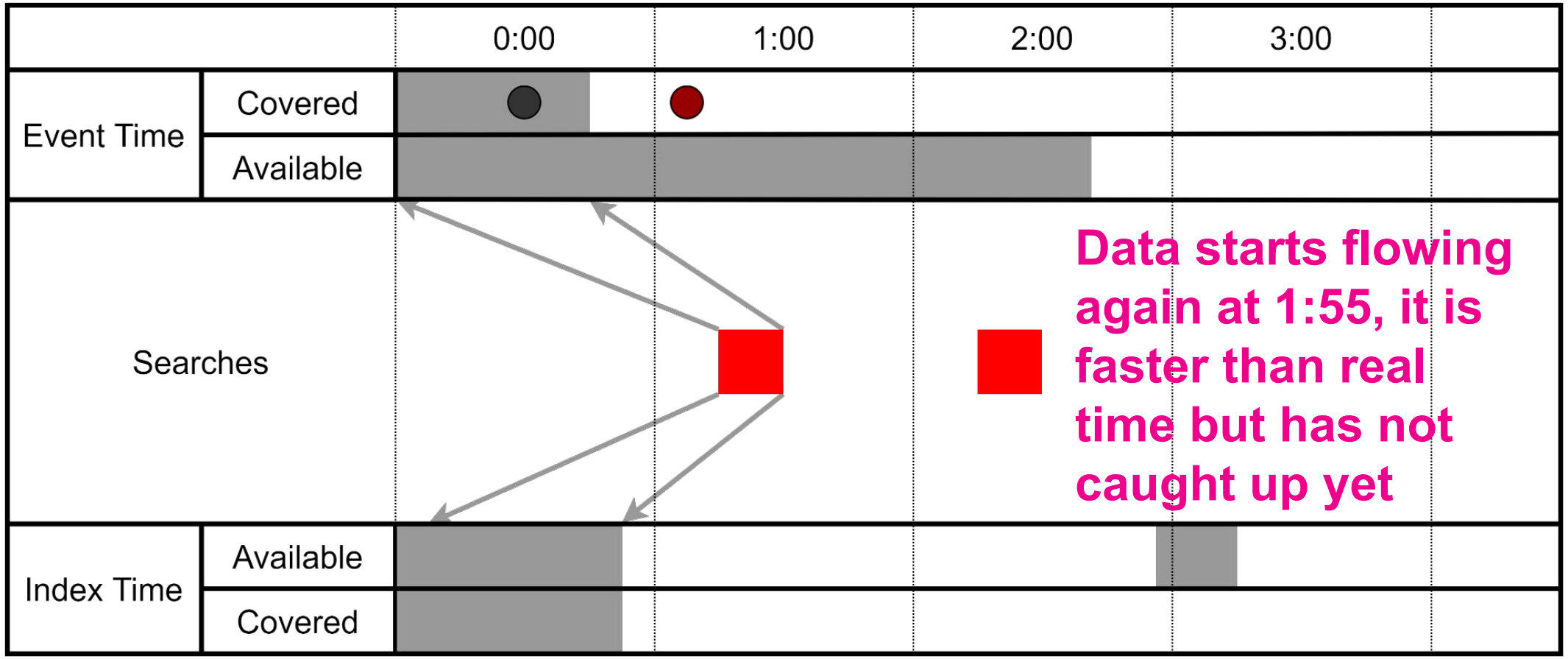
Latent Data | Index Time / Macro Method



Time: 02:10

Alerts Raised: 1 of 2

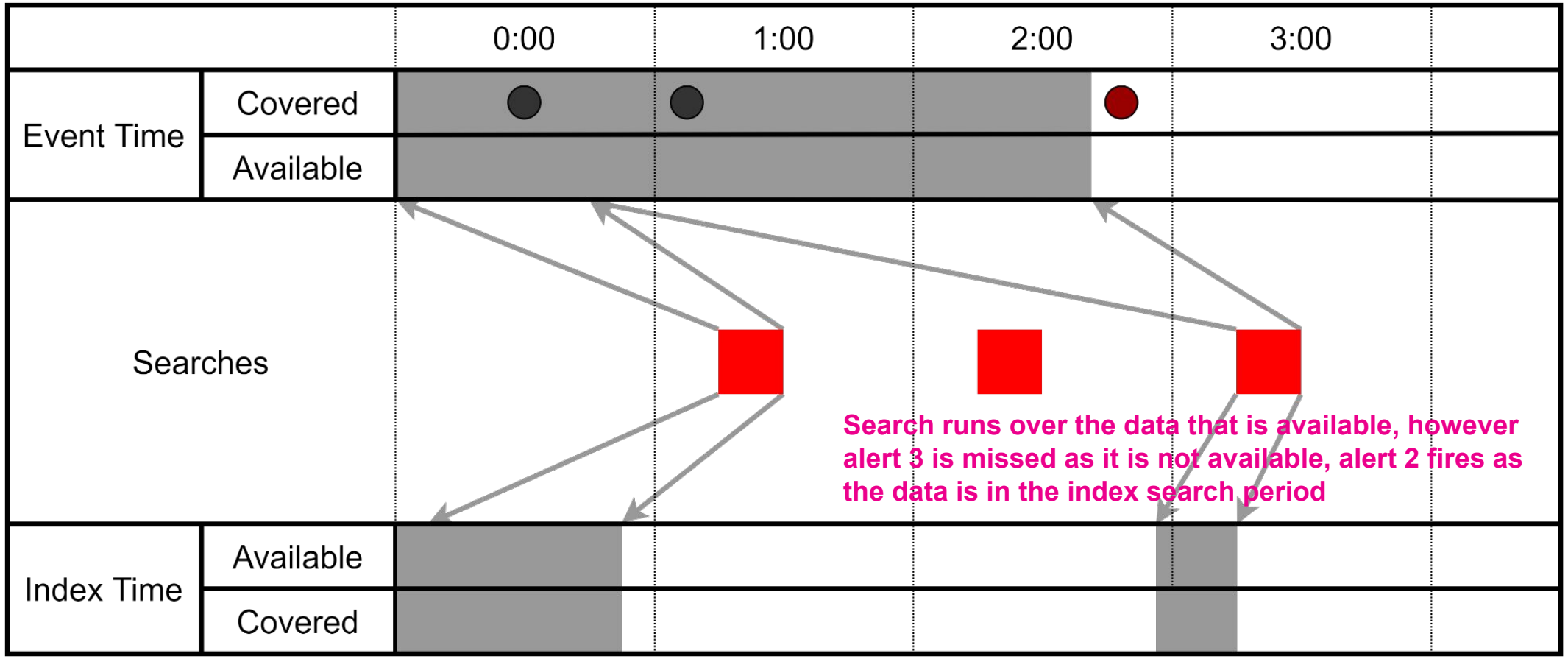
Latent Data | Index Time / Macro Method



Time: 03:10

Alerts Raised: 1 of 2

Latent Data | Index Time / Macro Method

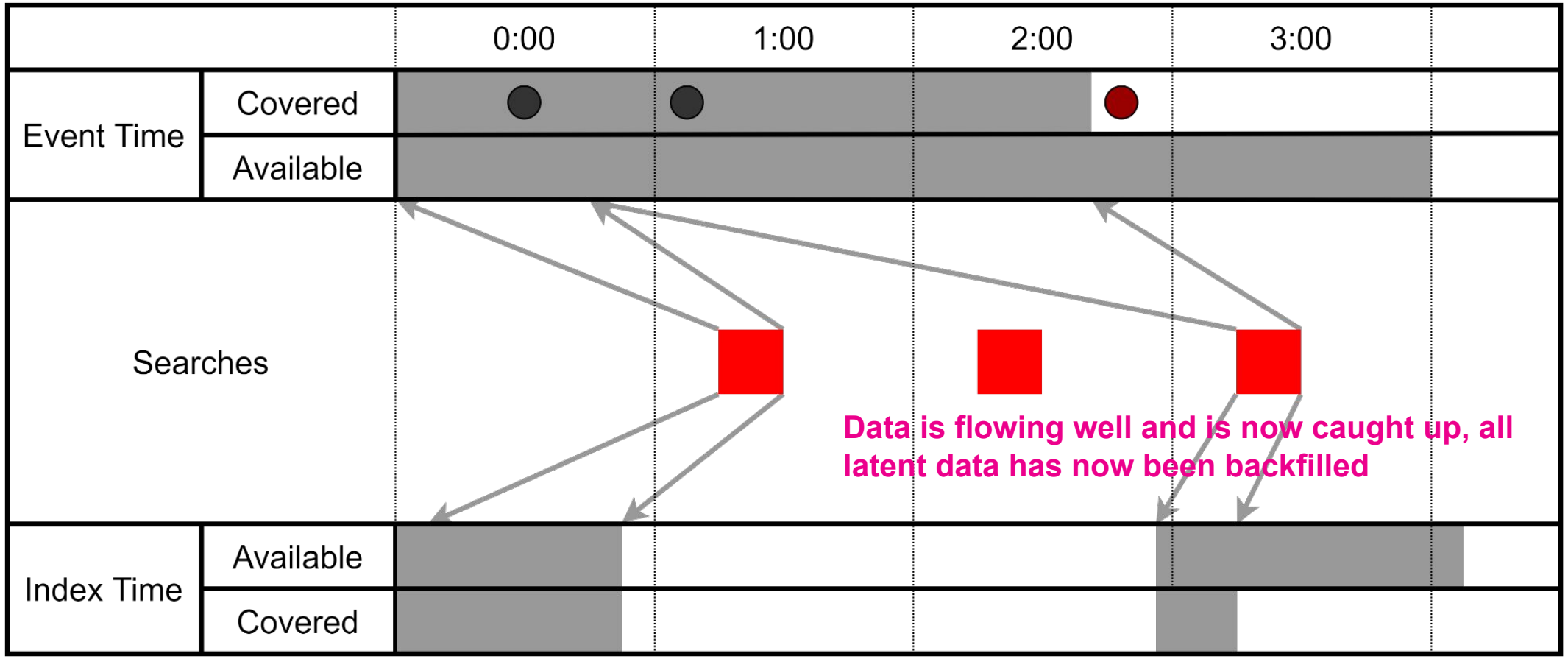


Time: 03:10

Alerts Raised: 2 of 3

splunk> .conf21

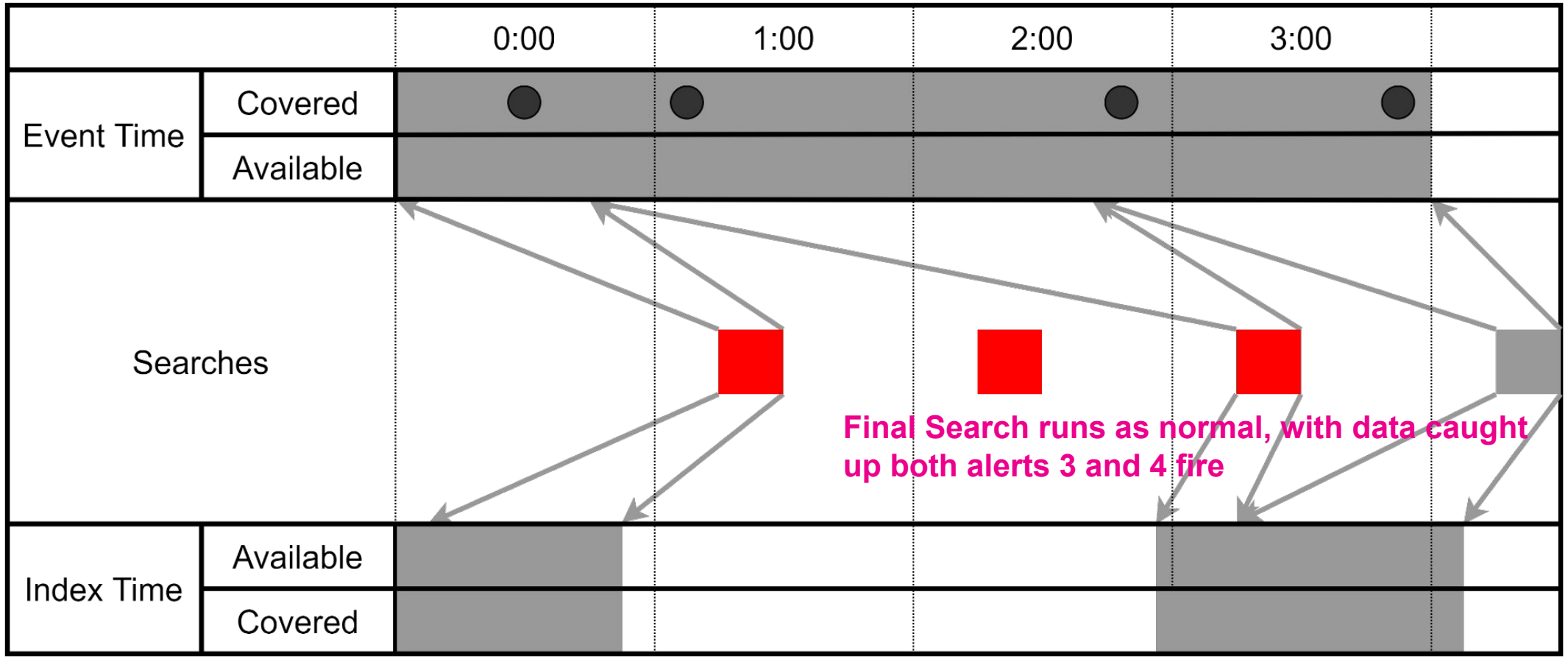
Latent Data | Index Time / Macro Method



Time: 04:10

Alerts Raised: 2 of 3

Latent Data | Index Time / Macro Method



Time: 04:10

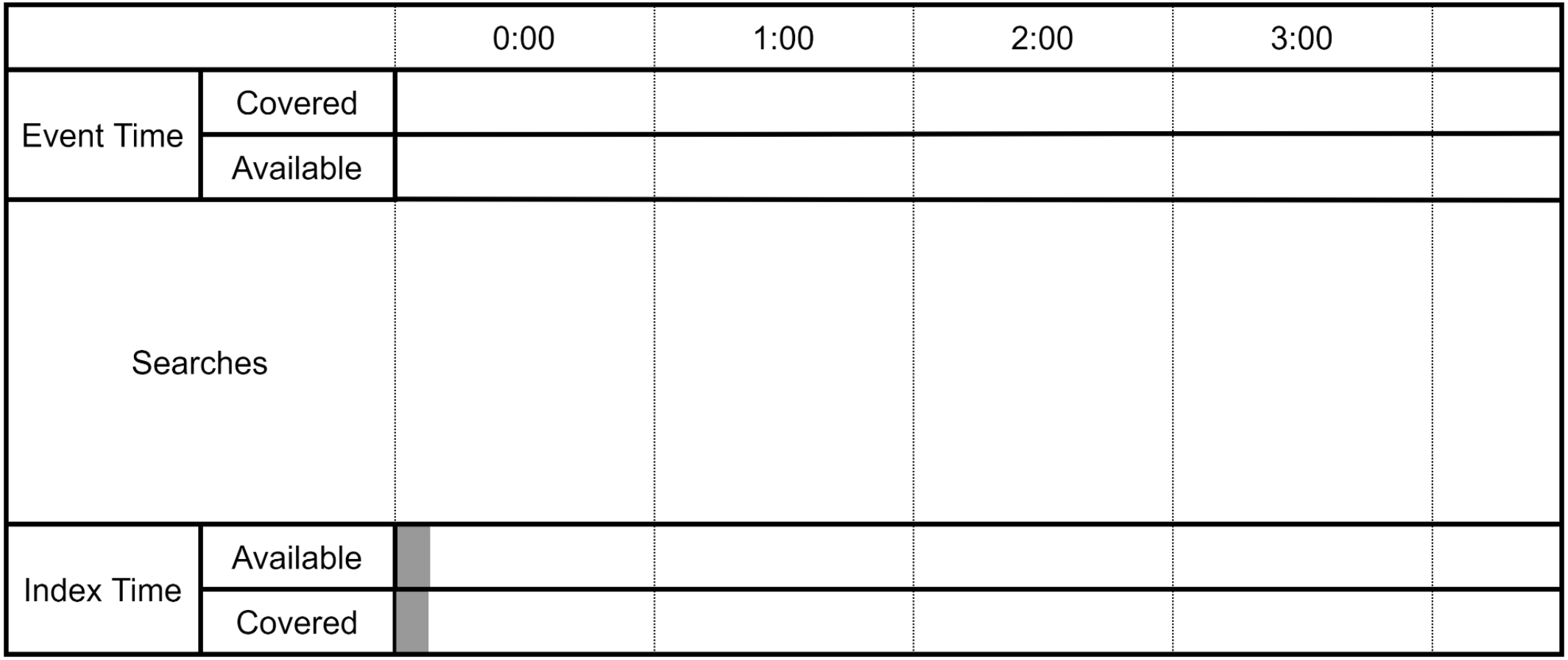
Alerts Raised: 4 of 4

splunk> .conf21

Scenario: Skipped Searches / SH Issues

Time Source: Index Time Searching

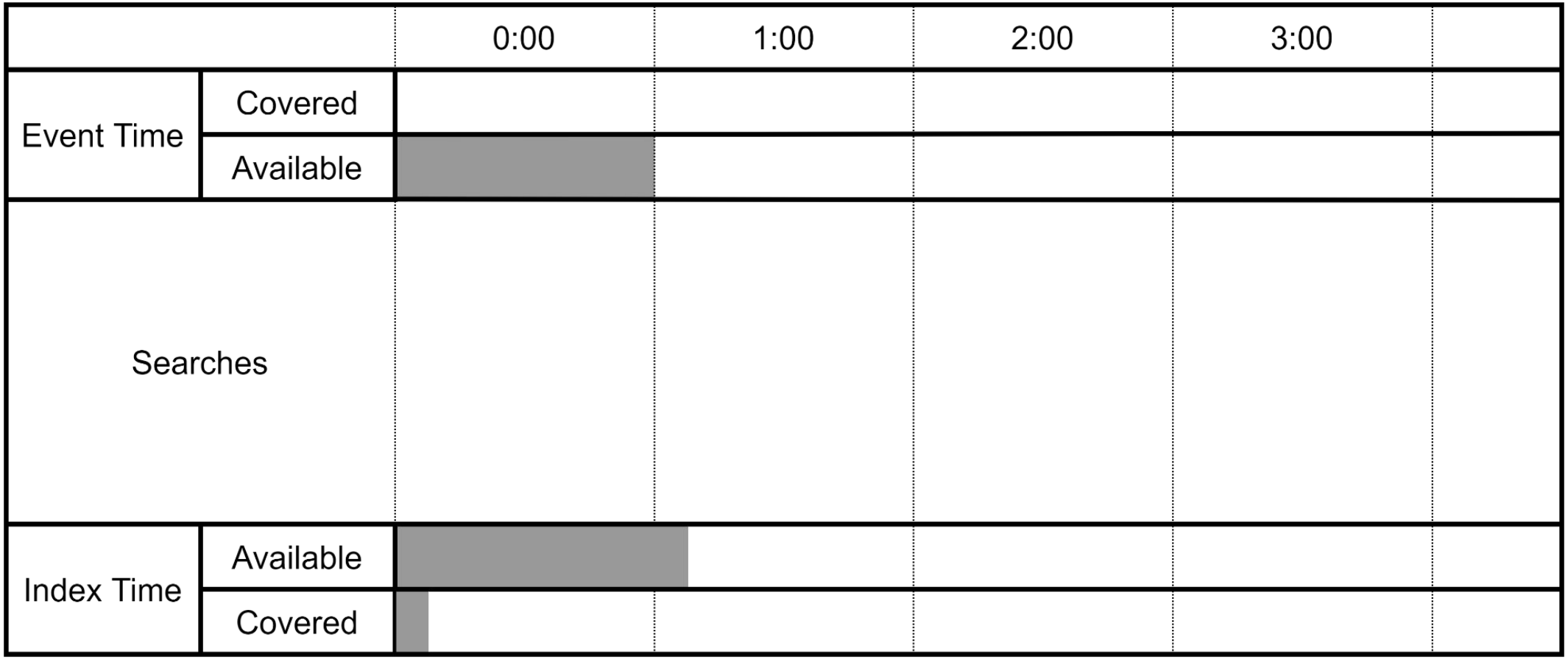
Skipped Search / SH Down / Issues | Index Time



Time: 00:10

Alerts Raised: 0 of 0

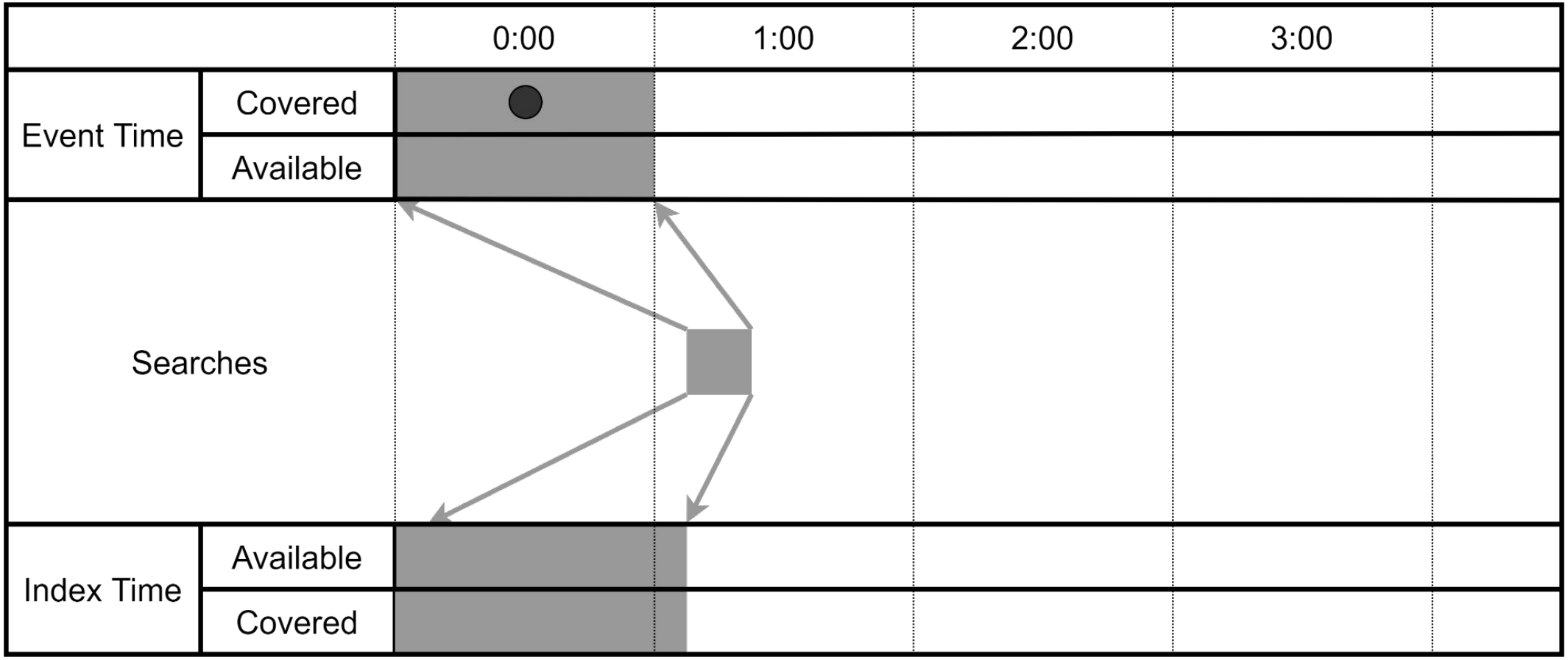
Skipped Search / SH Down / Issues | Index Time



Time: 01:10

Alerts Raised: 0 of 0

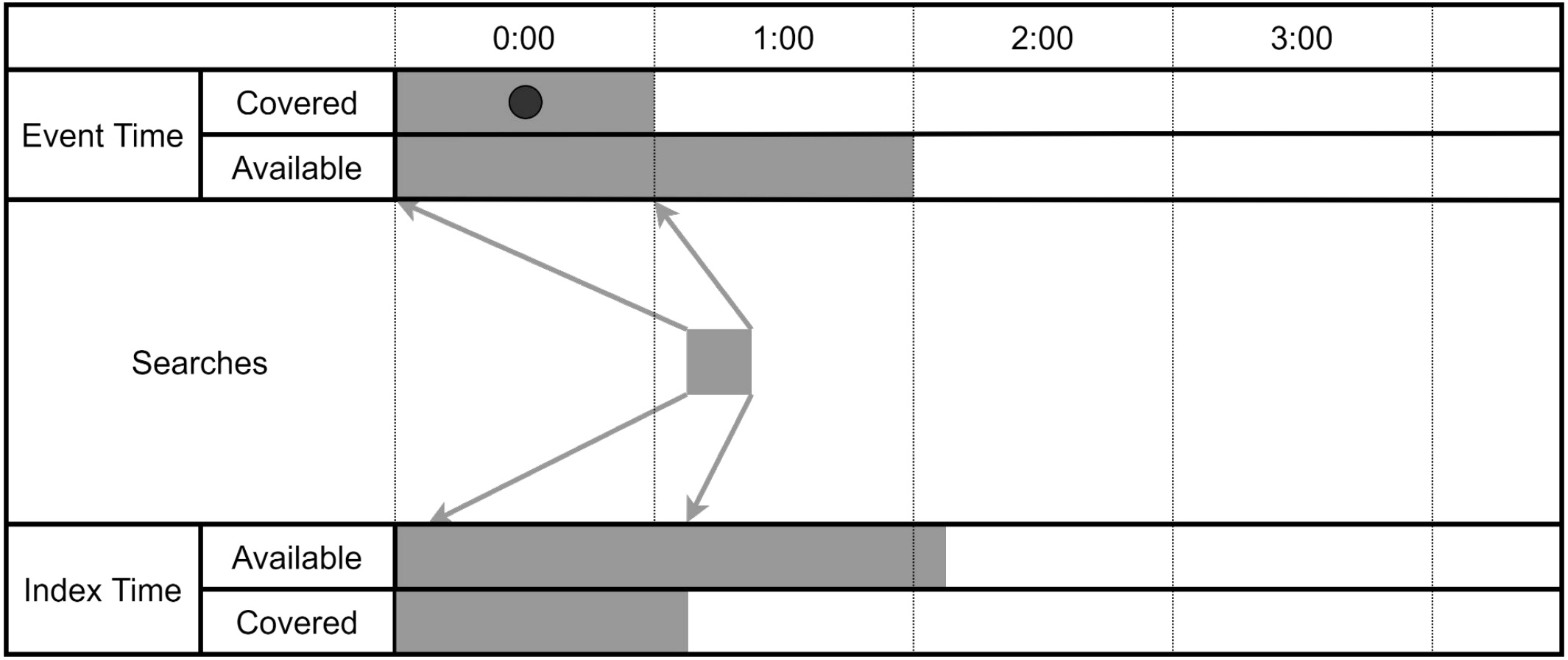
Skipped Search / SH Down / Issues | Index Time



Time: 01:10

Alerts Raised: 1 of 1

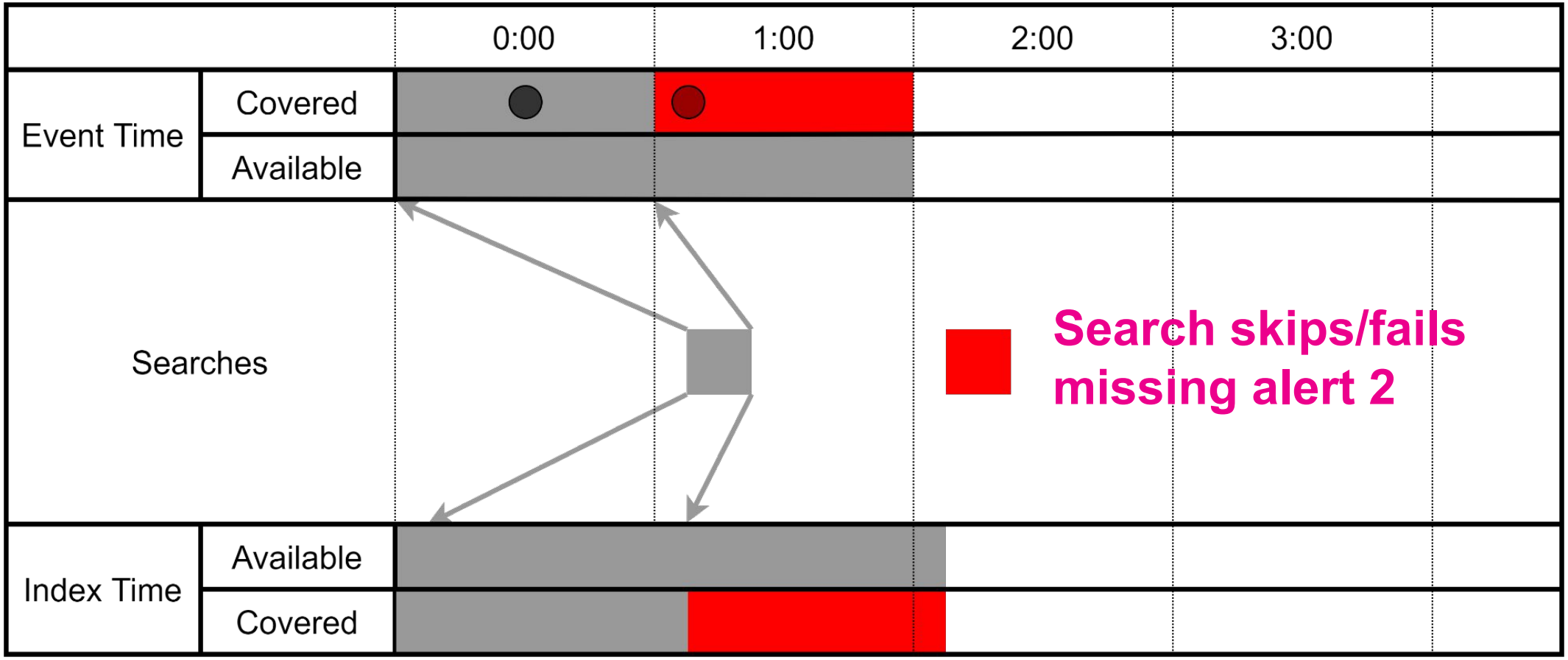
Skipped Search / SH Down / Issues | Index Time



Time: 02:10

Alerts Raised: 1 of 1

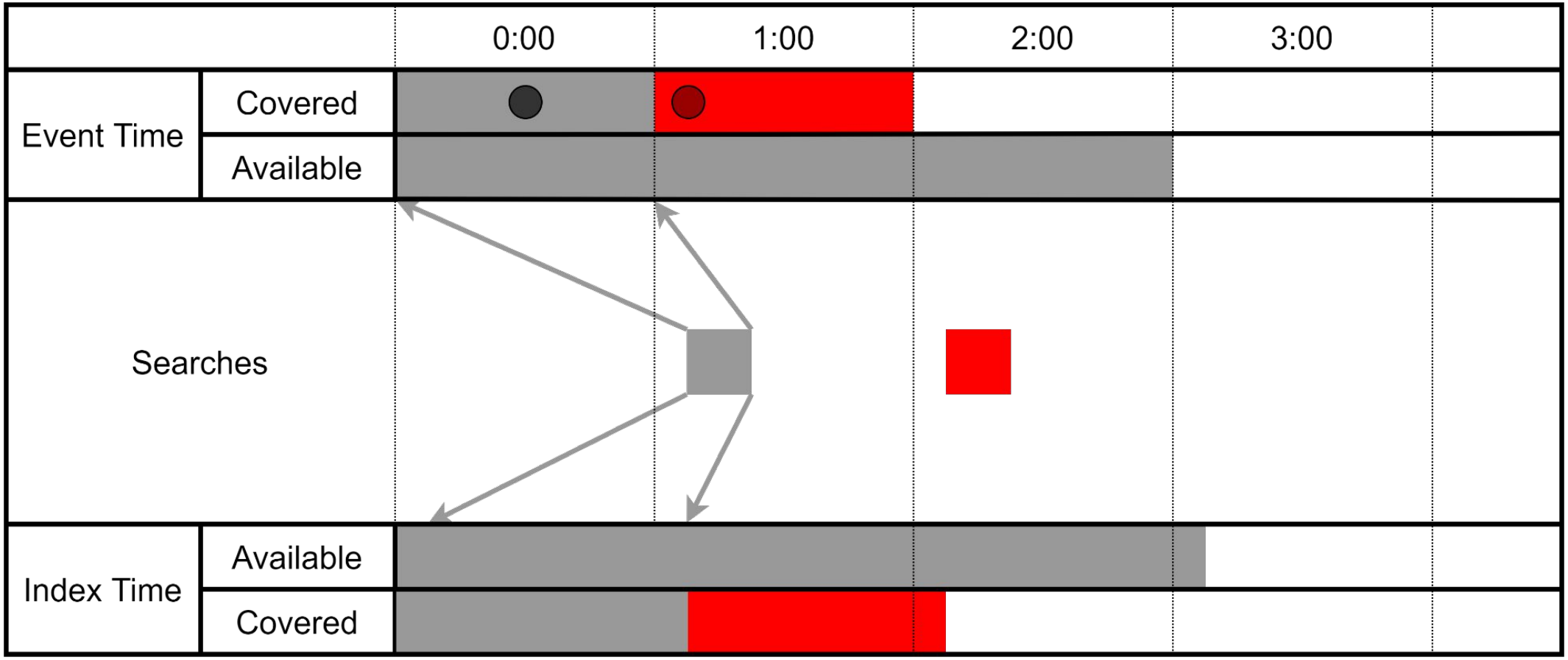
Skipped Search / SH Down / Issues | Index Time



Time: 02:10

Alerts Raised: 1 of 2

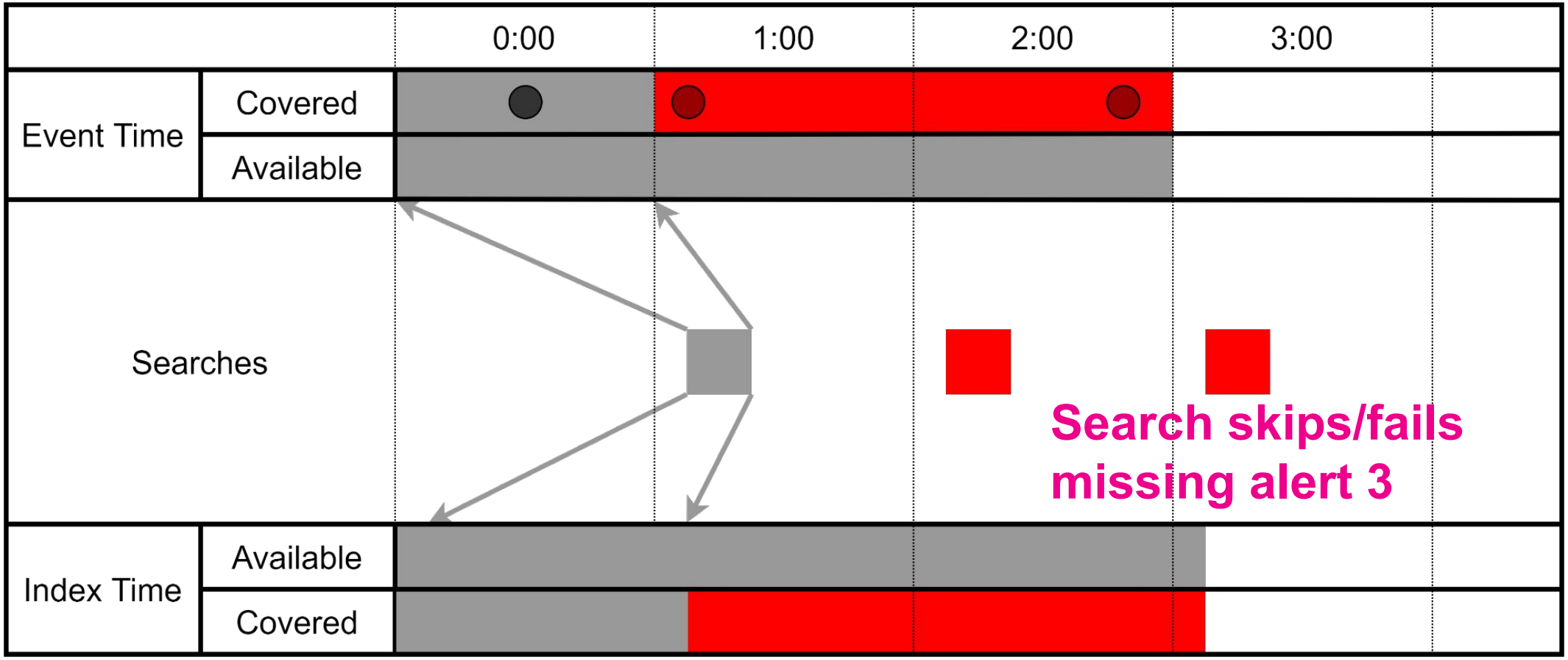
Skipped Search / SH Down / Issues | Index Time



Time: 03:10

Alerts Raised: 1 of 2

Skipped Search / SH Down / Issues | Index Time

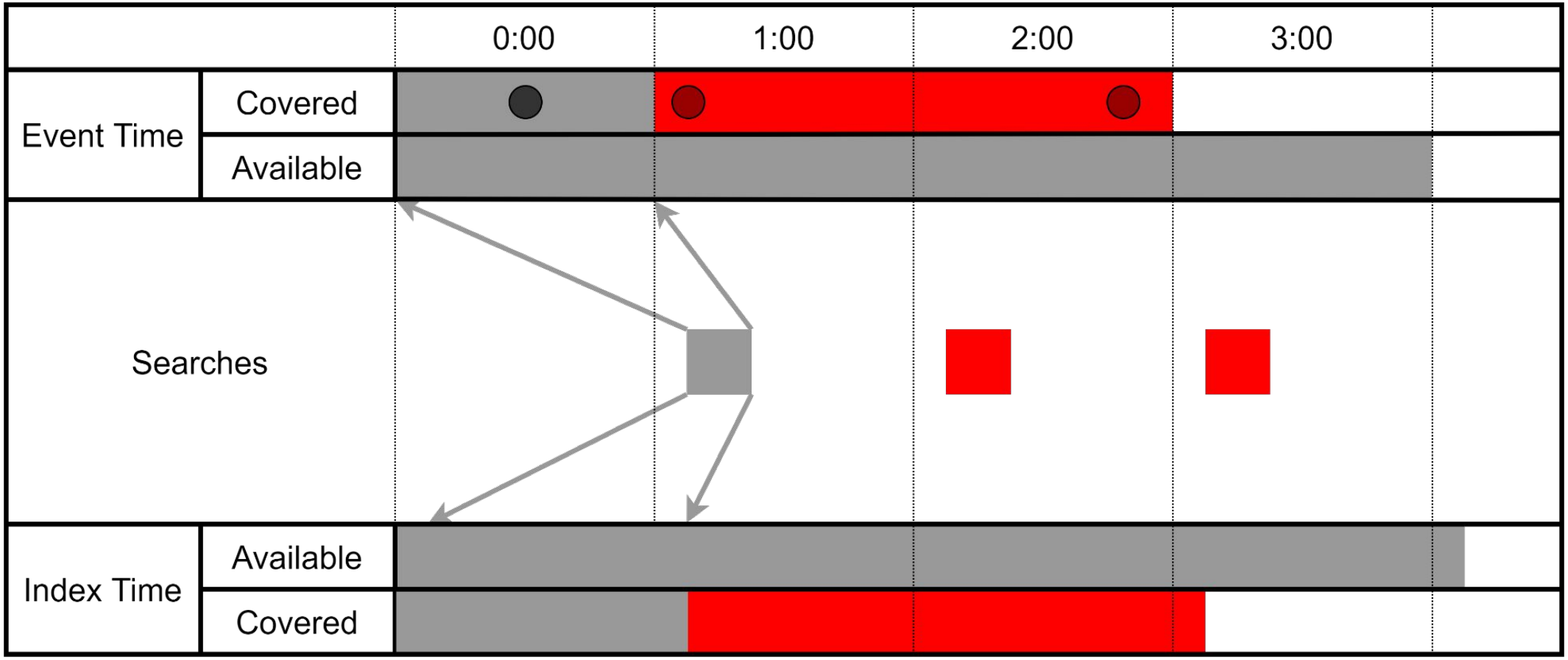


Time: 03:10

Alerts Raised: 1 of 3

splunk> .conf21

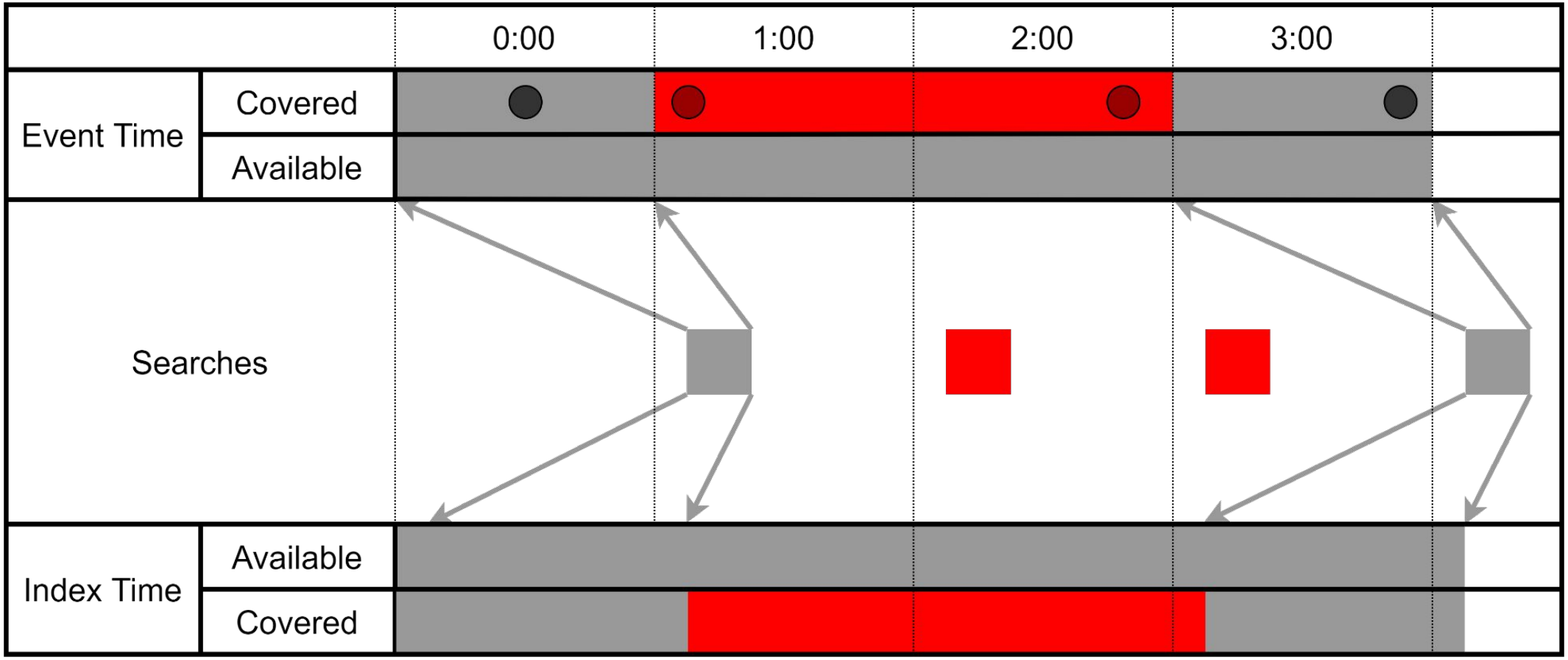
Skipped Search / SH Down / Issues | Index Time



Time: 04:10

Alerts Raised: 1 of 3

Skipped Search / SH Down / Issues | Index Time



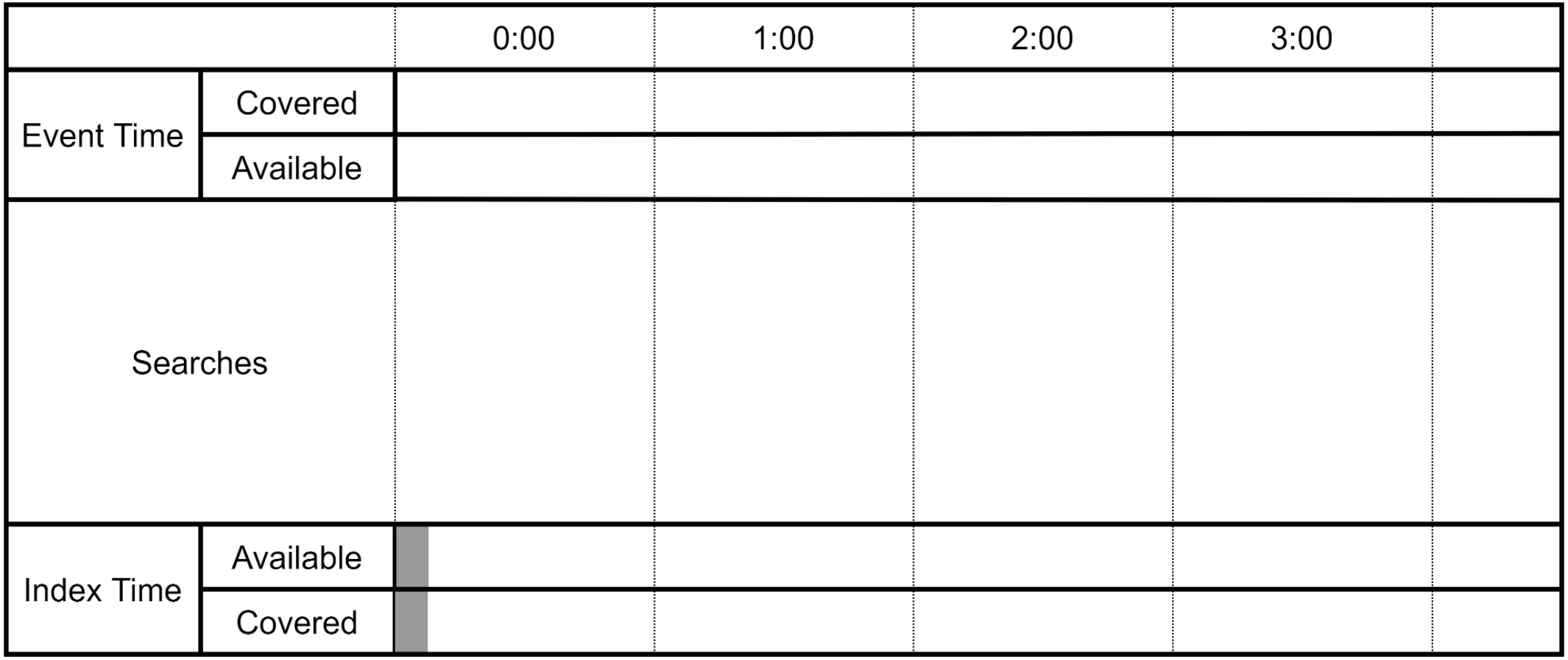
Time: 04:10

Alerts Raised: 2 of 4

Scenario: Skipped Searches / SH Issues

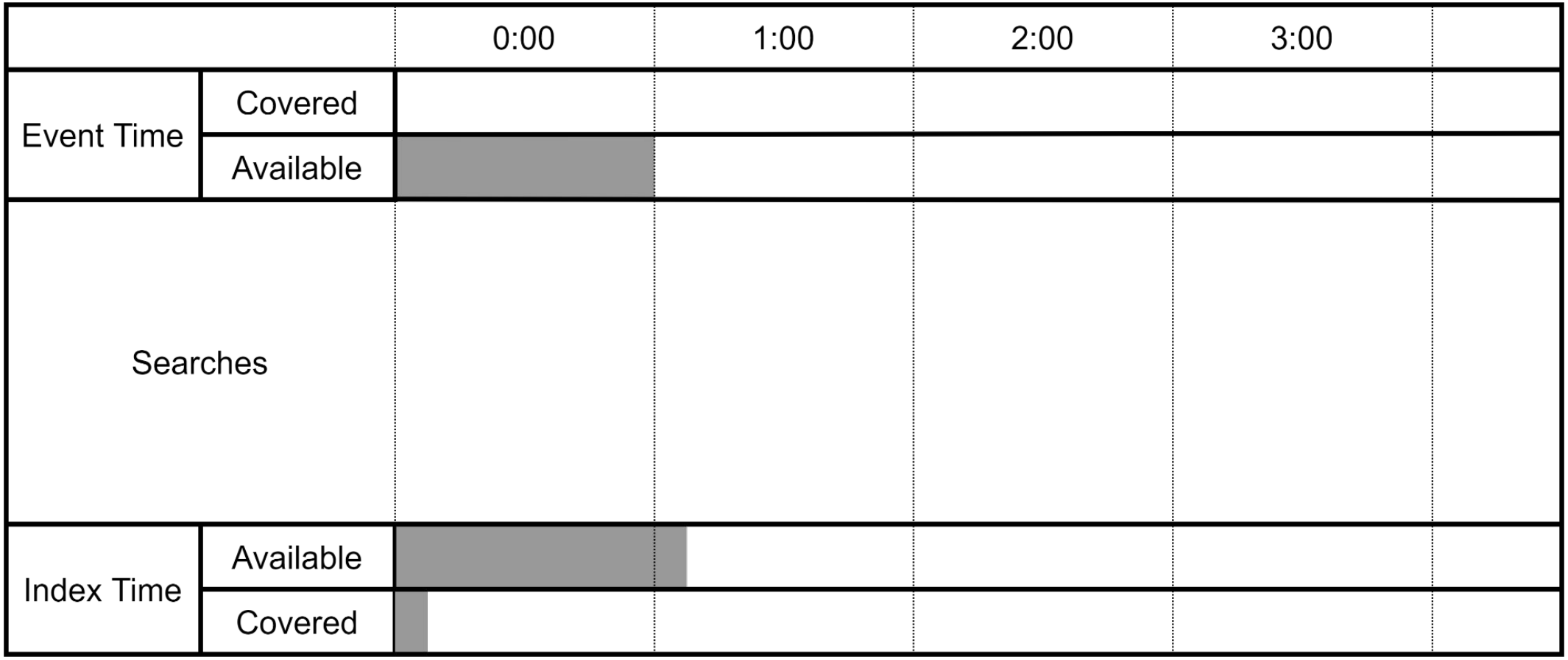
Time Source: Macro Method Searching

Skipped Search / SH Down / Issues | Macro Method



Time: 00:10 **Last Run: 00:10** **Alerts Raised: 0 of 0**

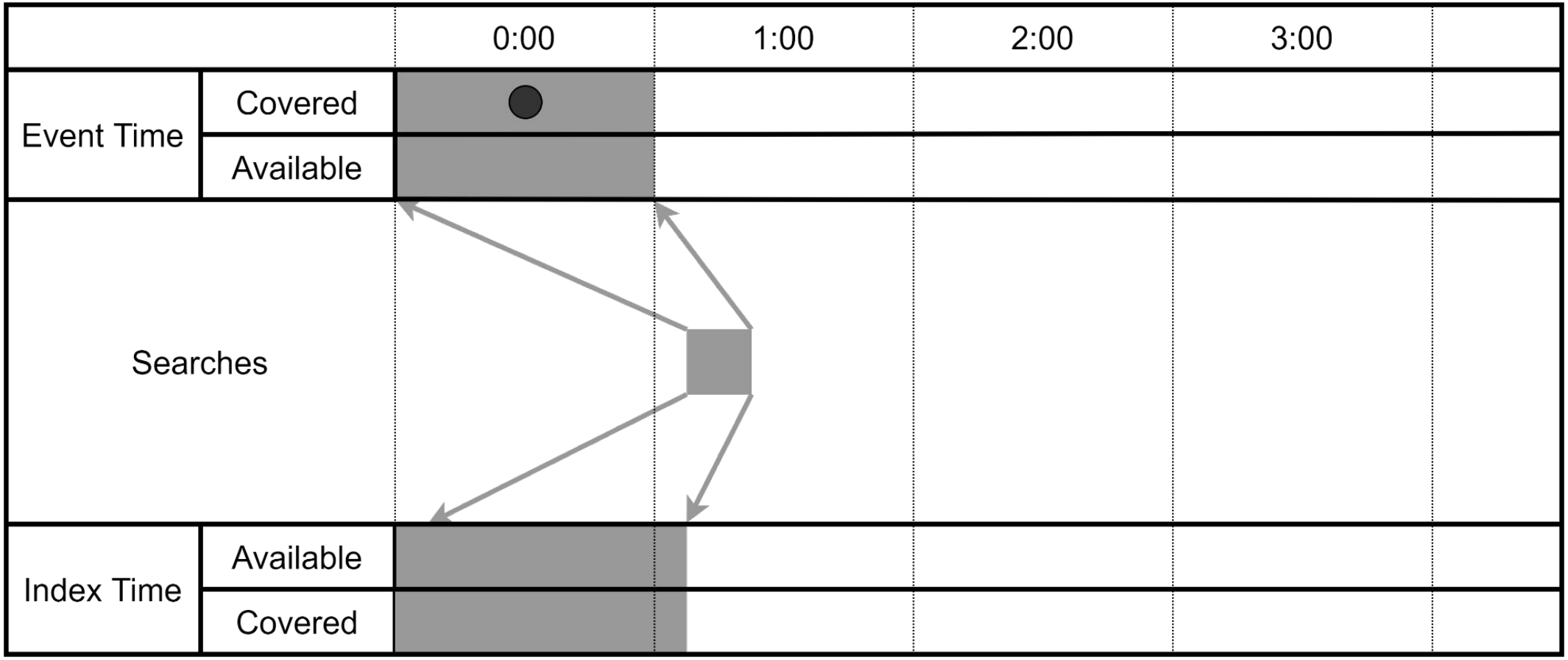
Skipped Search / SH Down / Issues | Macro Method



Time: 01:10 **Last Run: 00:10** **Alerts Raised: 0 of 0**

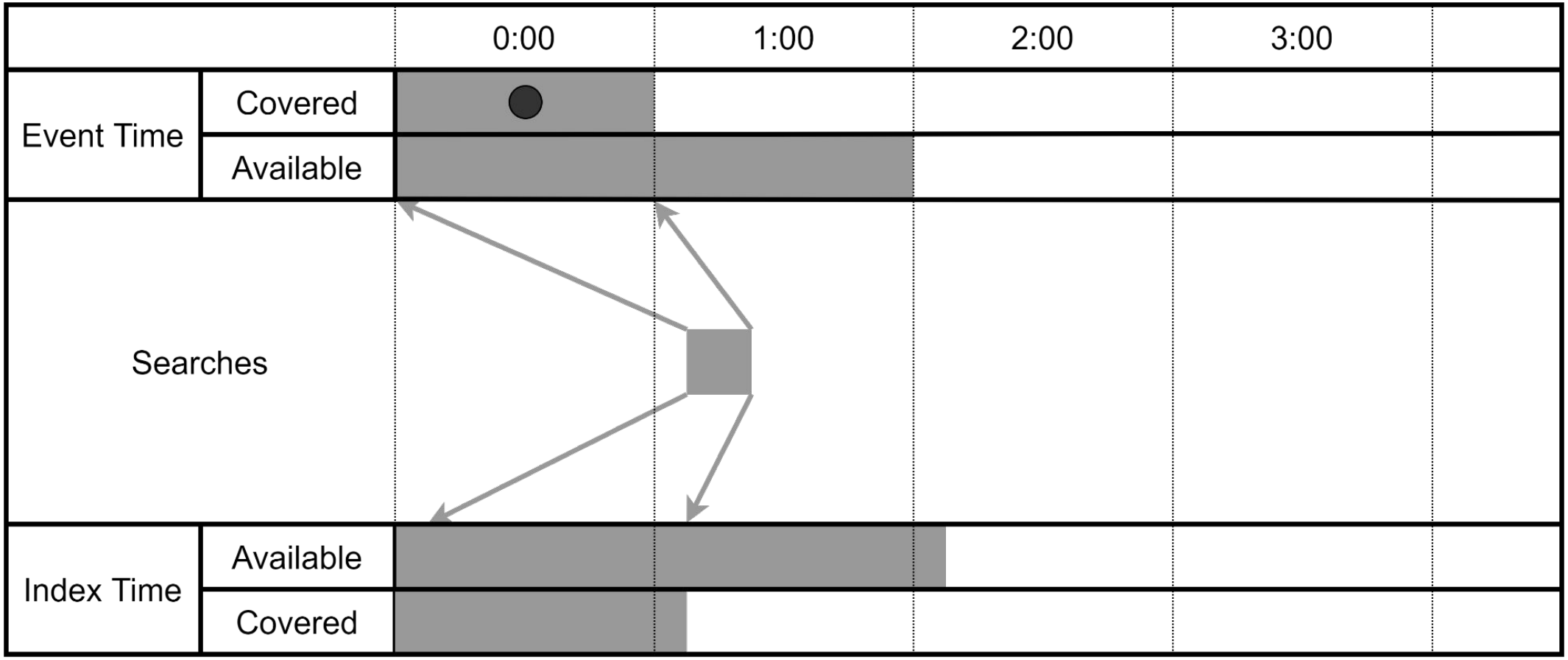
splunk> .conf21

Skipped Search / SH Down / Issues | Macro Method



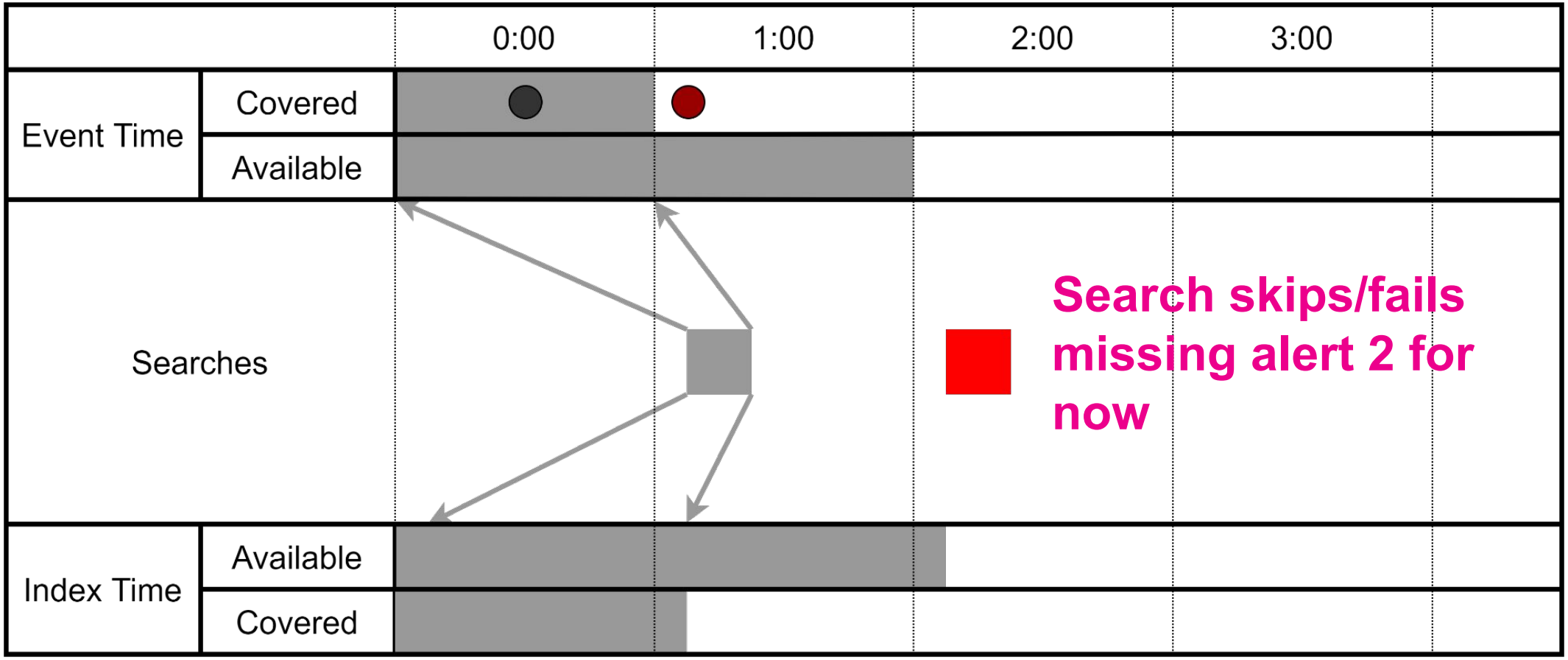
Time: 01:10 **Last Run: 01:10** **Alerts Raised: 1 of 1**

Skipped Search / SH Down / Issues | Macro Method



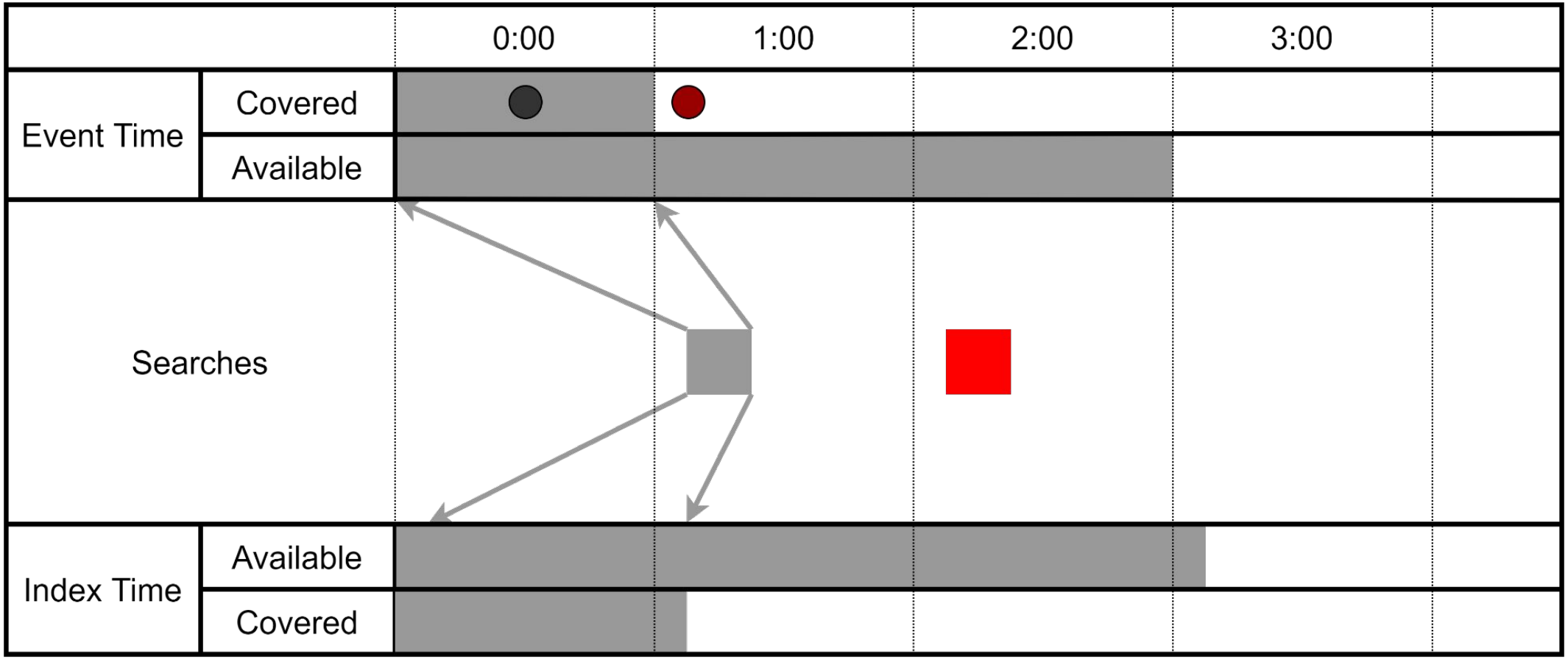
Time: 02:10 **Last Run: 01:10** **Alerts Raised: 1 of 1**

Skipped Search / SH Down / Issues | Macro Method



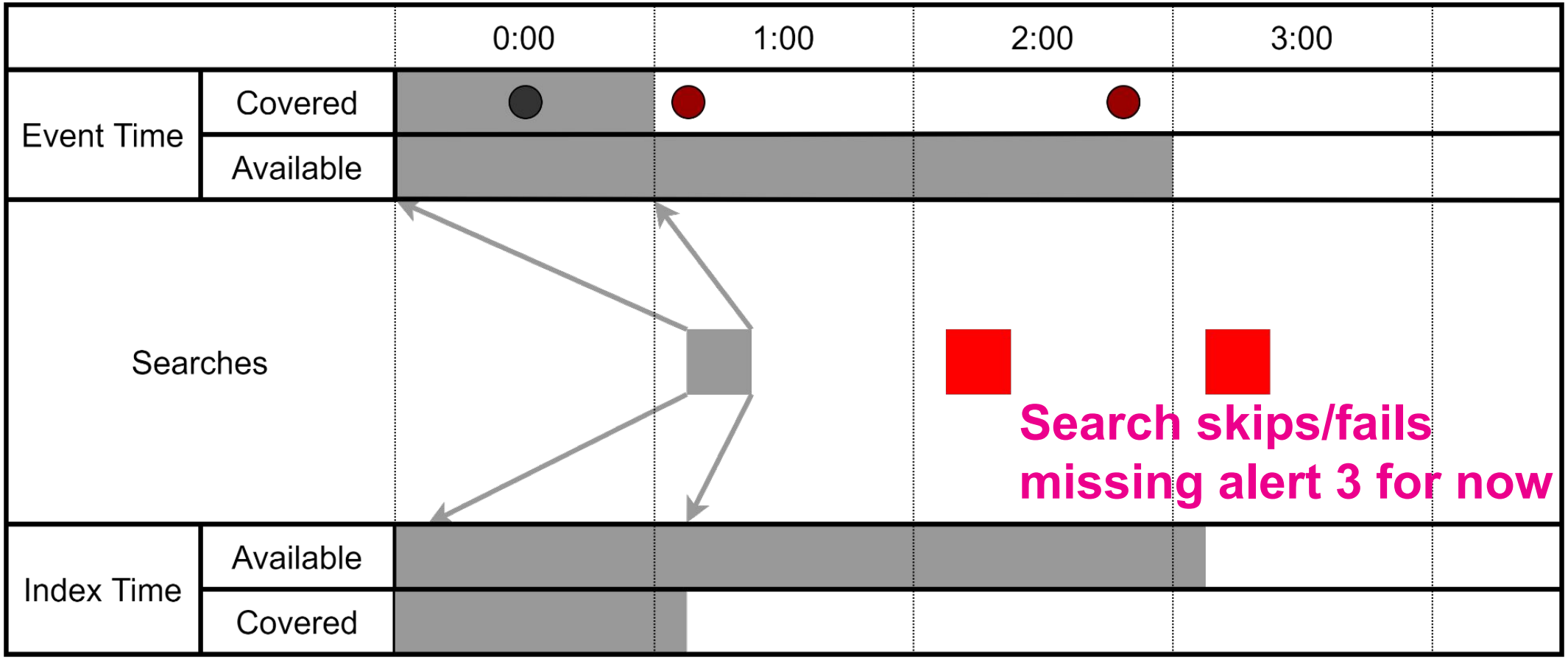
Time: 02:10 **Last Run: 01:10** **Alerts Raised: 1 of 2**

Skipped Search / SH Down / Issues | Macro Method



Time: 03:10 **Last Run: 01:10** **Alerts Raised: 1 of 2**

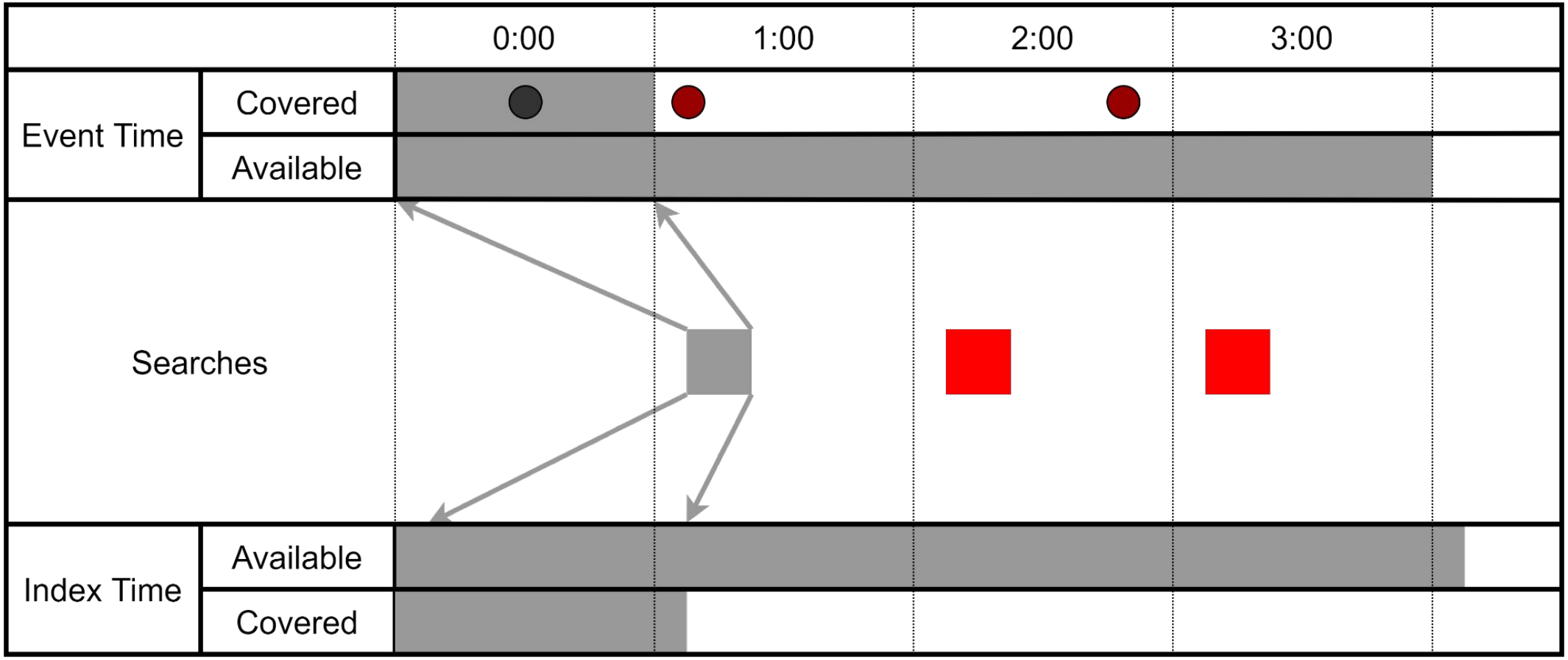
Skipped Search / SH Down / Issues | Macro Method



Time: 03:10 **Last Run: 01:10** **Alerts Raised: 1 of 3**

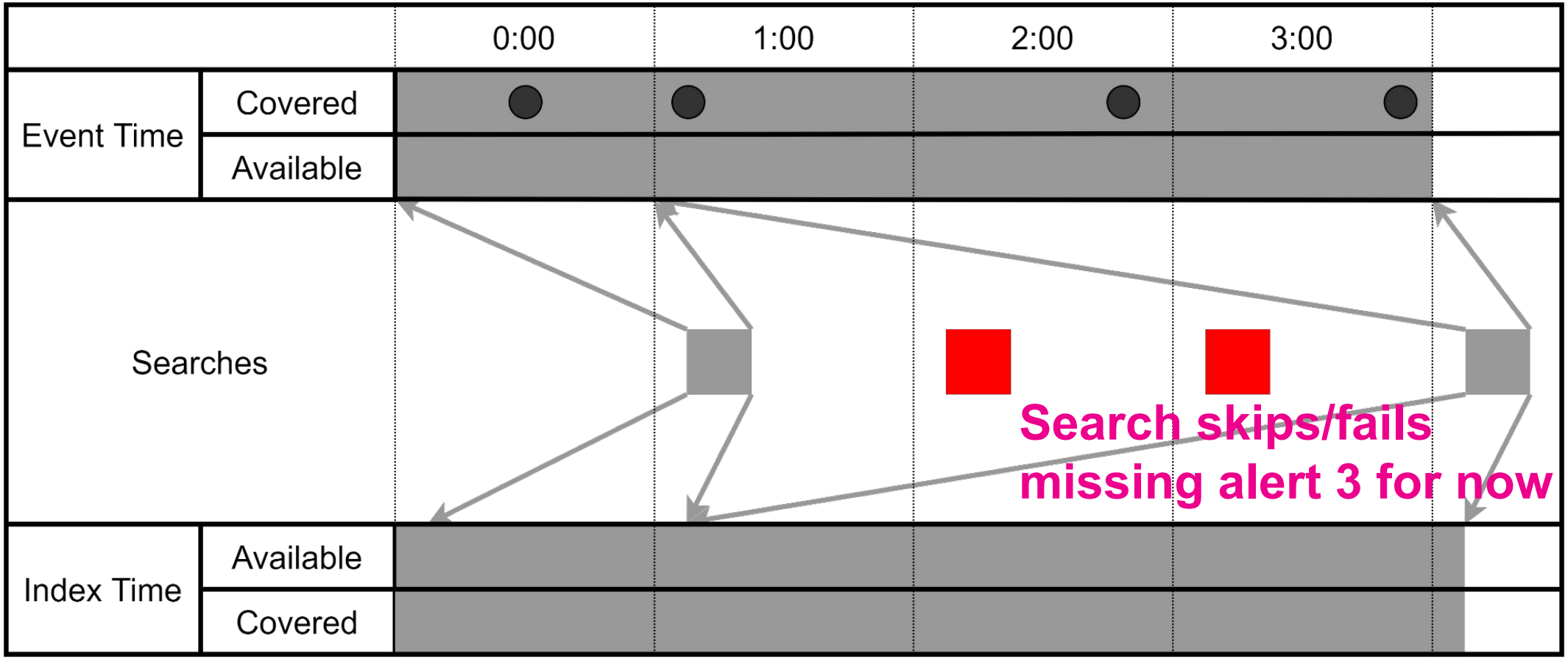
splunk> .conf21

Skipped Search / SH Down / Issues | Macro Method



Time: 04:10 **Last Run: 01:10** **Alerts Raised: 1 of 3**

Skipped Search / SH Down / Issues | Macro Method



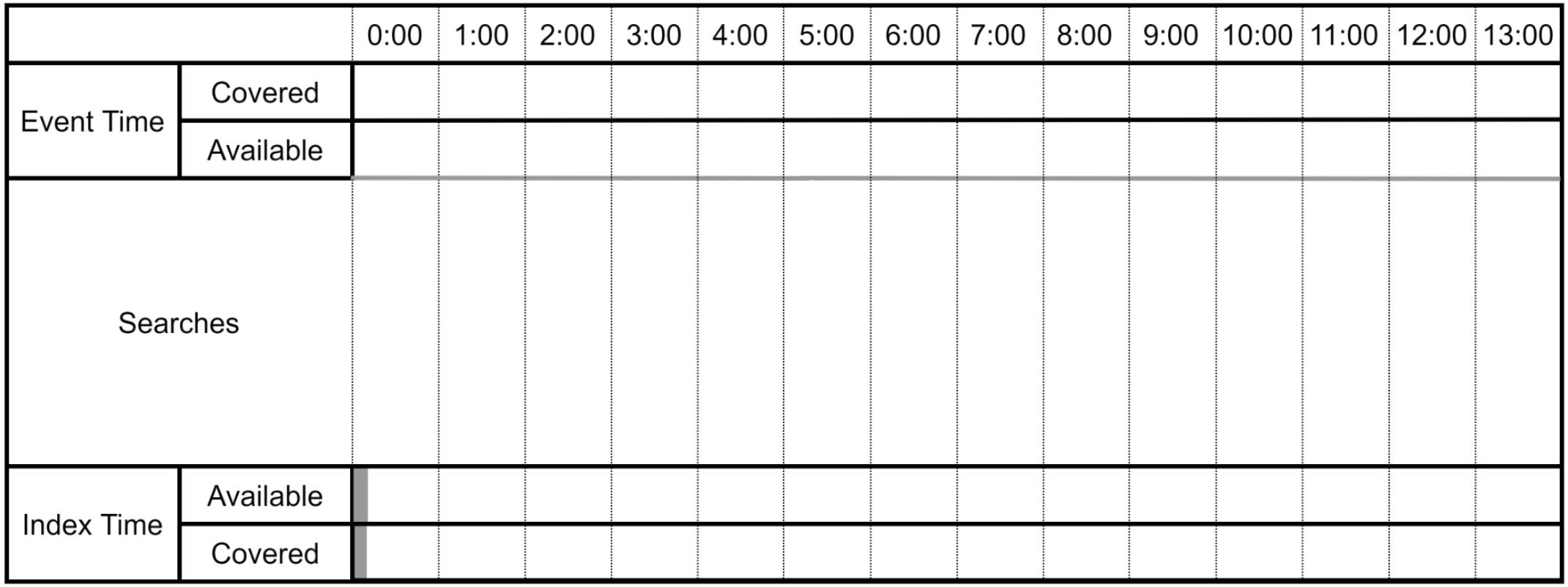
Time: 04:10 **Last Run: 04:10** **Alerts Raised: 4 of 4**

splunk> .conf21

Scenario: Skipped Searches / SH Issues Longer Time Period

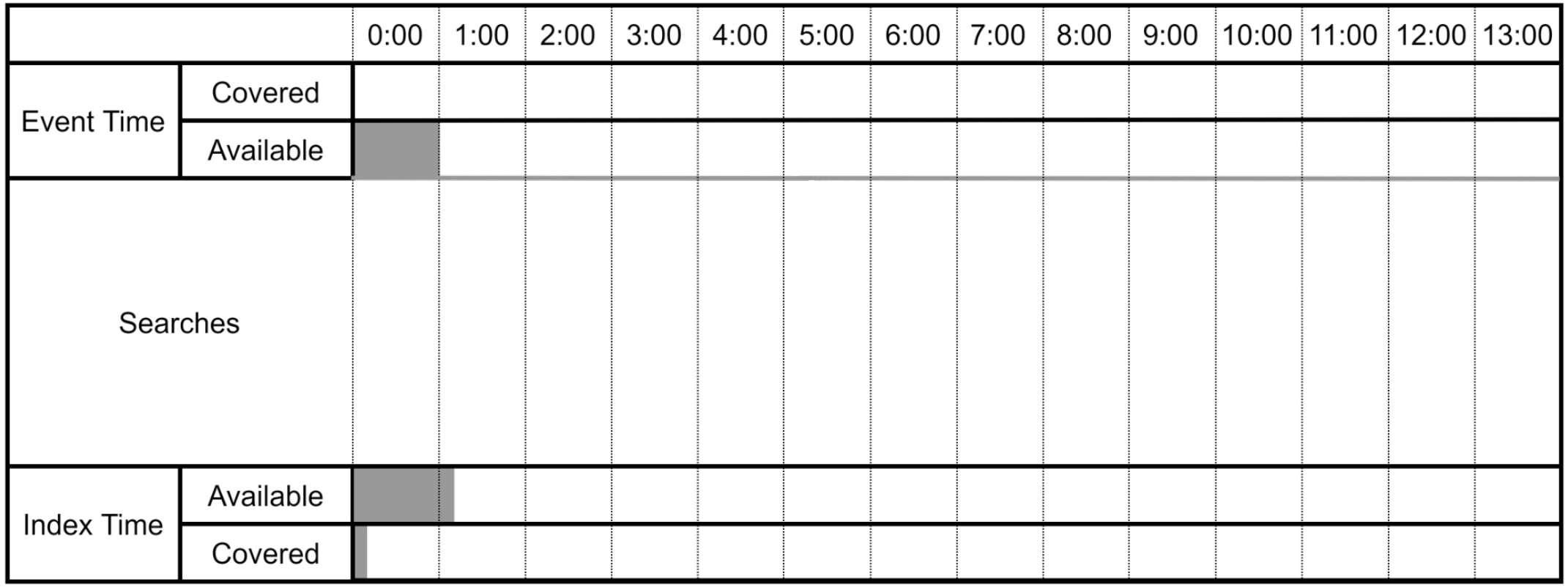
Time Source: Macro Method Searching

Skipped Search / SH Down / Issues | Macro Method



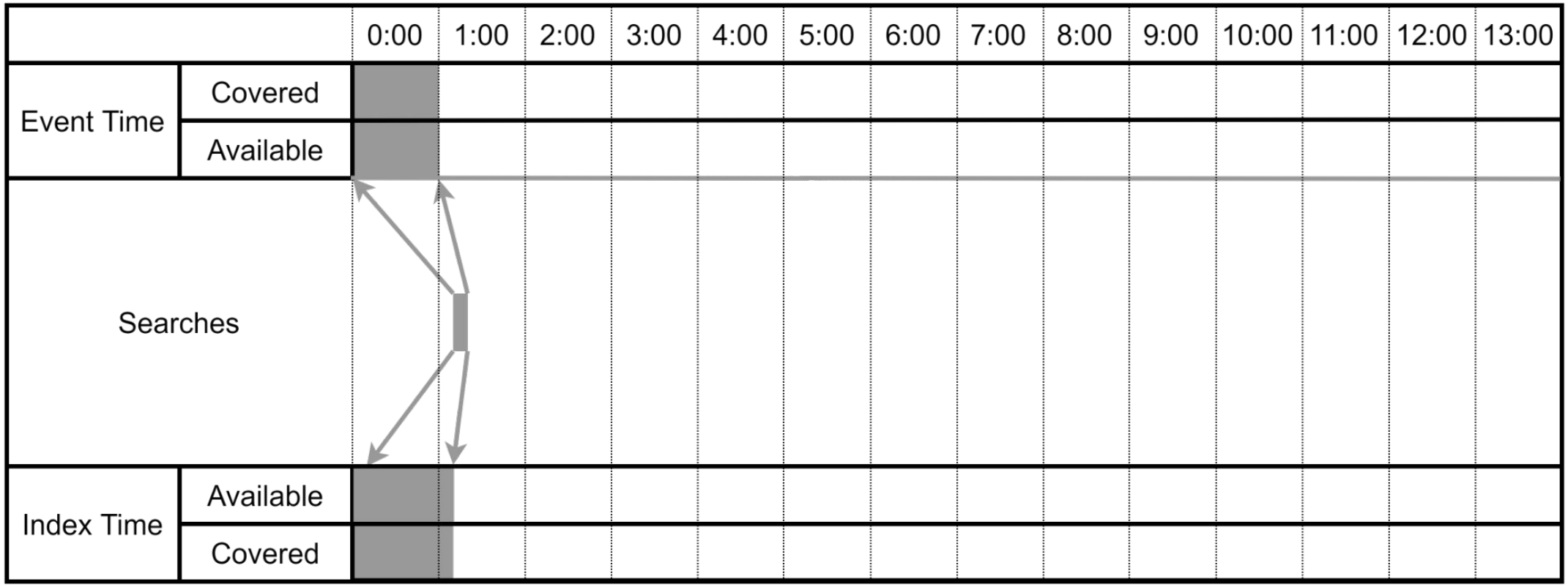
Time: 00:10 **Last Run: 00:10**

Skipped Search / SH Down / Issues | Macro Method



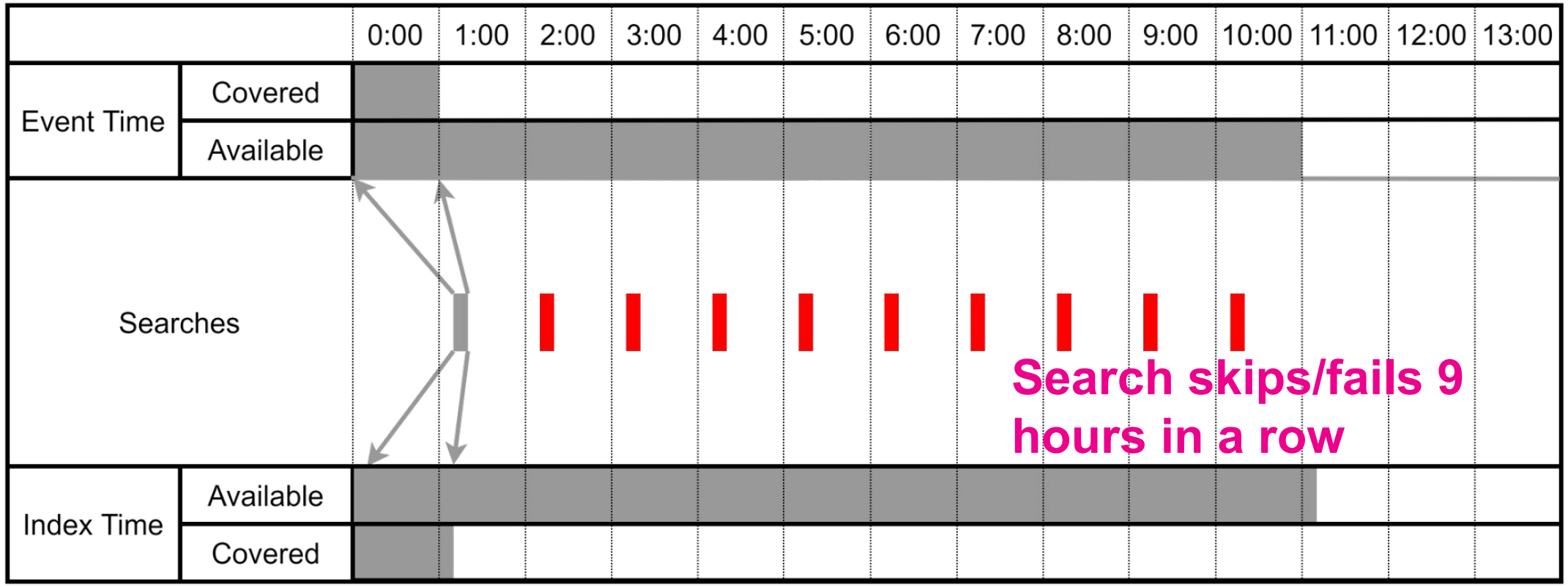
Time: 01:10 **Last Run: 00:10**

Skipped Search / SH Down / Issues | Macro Method



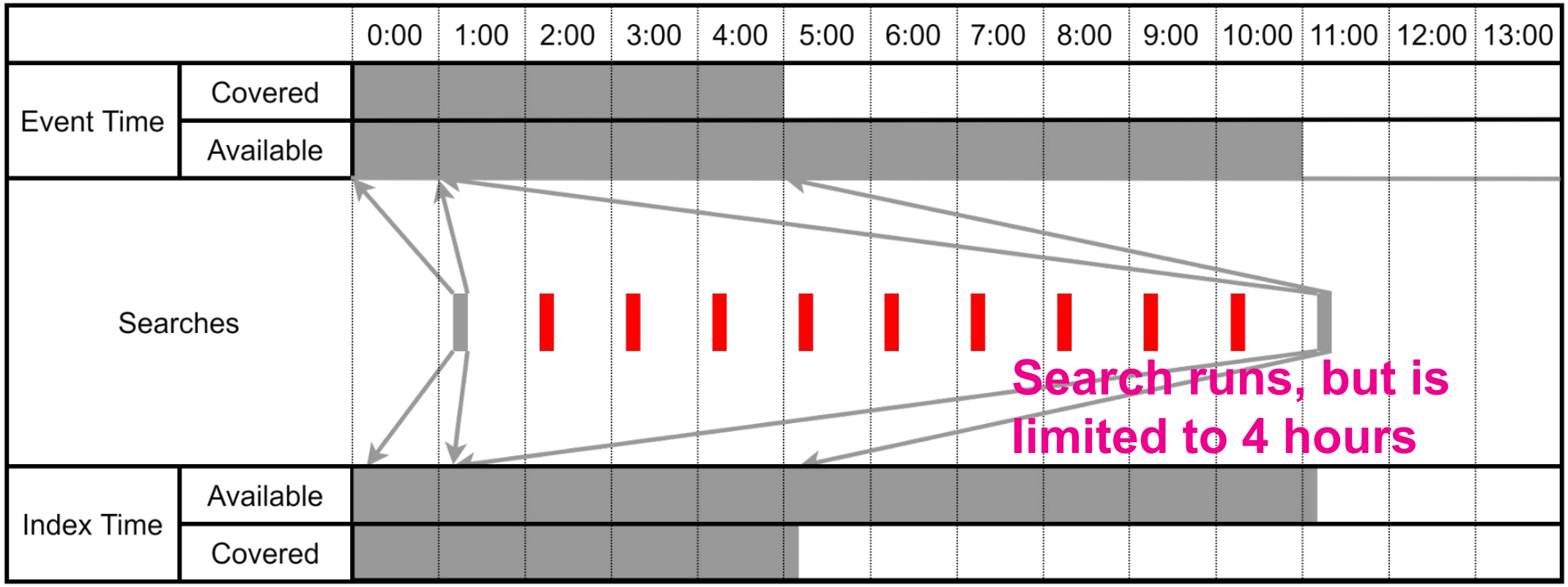
Time: 01:10 **Last Run: 01:10**

Skipped Search / SH Down / Issues | Macro Method



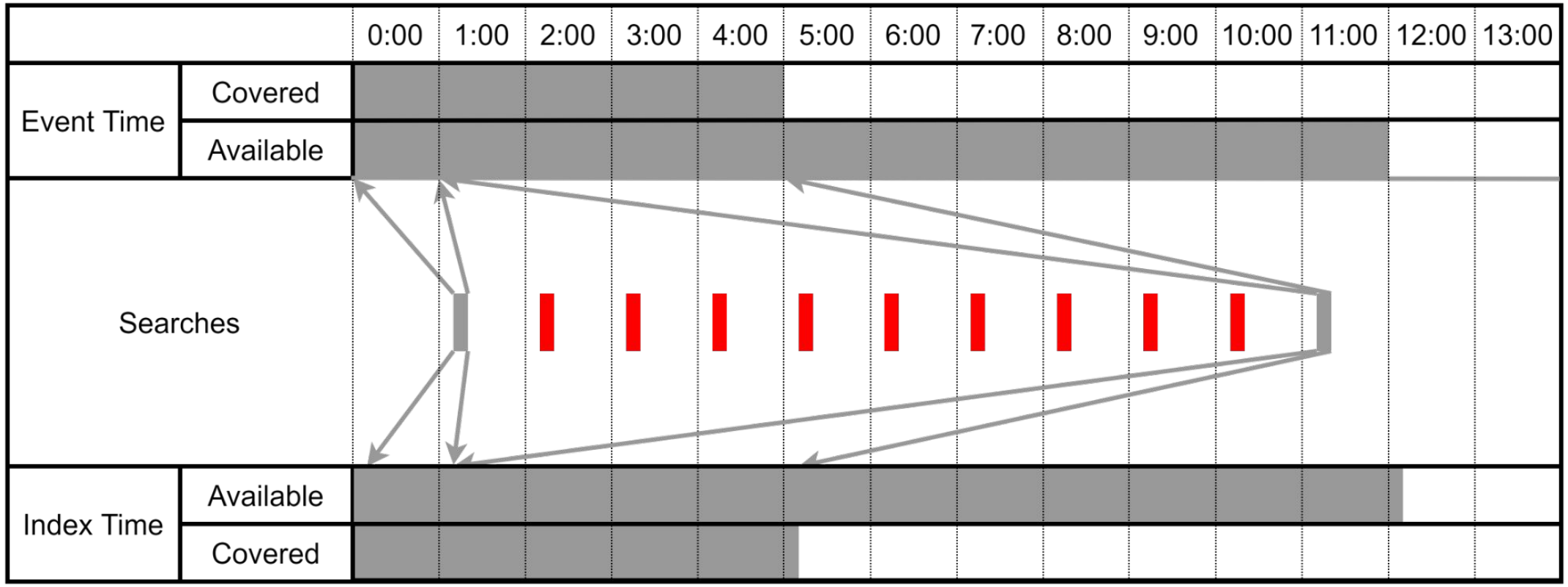
Time: 11:10 **Last Run: 01:10**

Skipped Search / SH Down / Issues | Macro Method



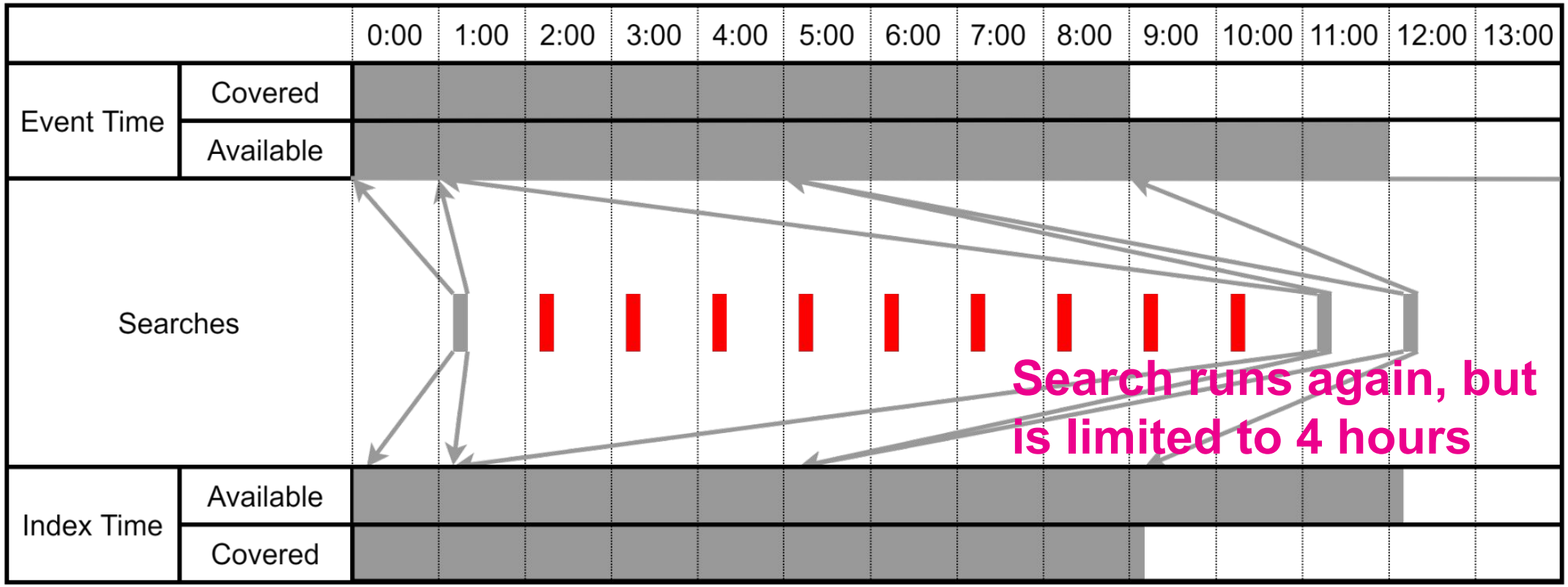
Time: 11:10 **Last Run: 05:10**

Skipped Search / SH Down / Issues | Macro Method



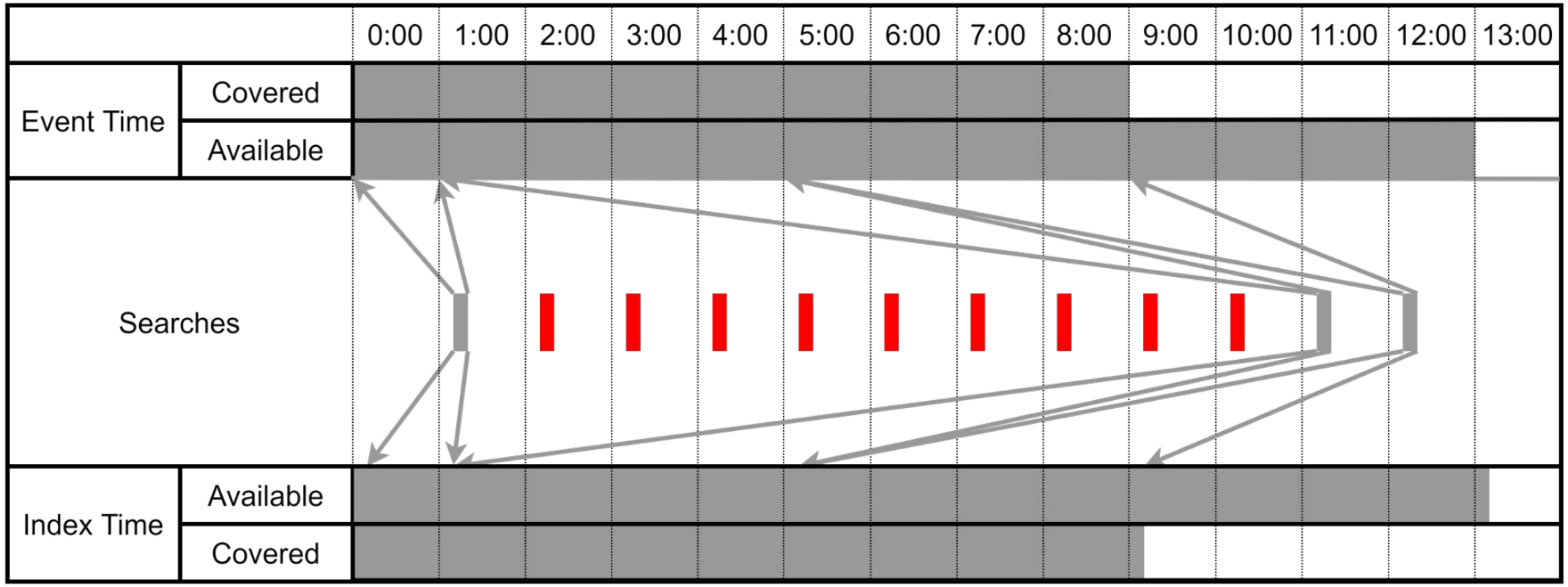
Time: 12:10 **Last Run: 05:10**

Skipped Search / SH Down / Issues | Macro Method



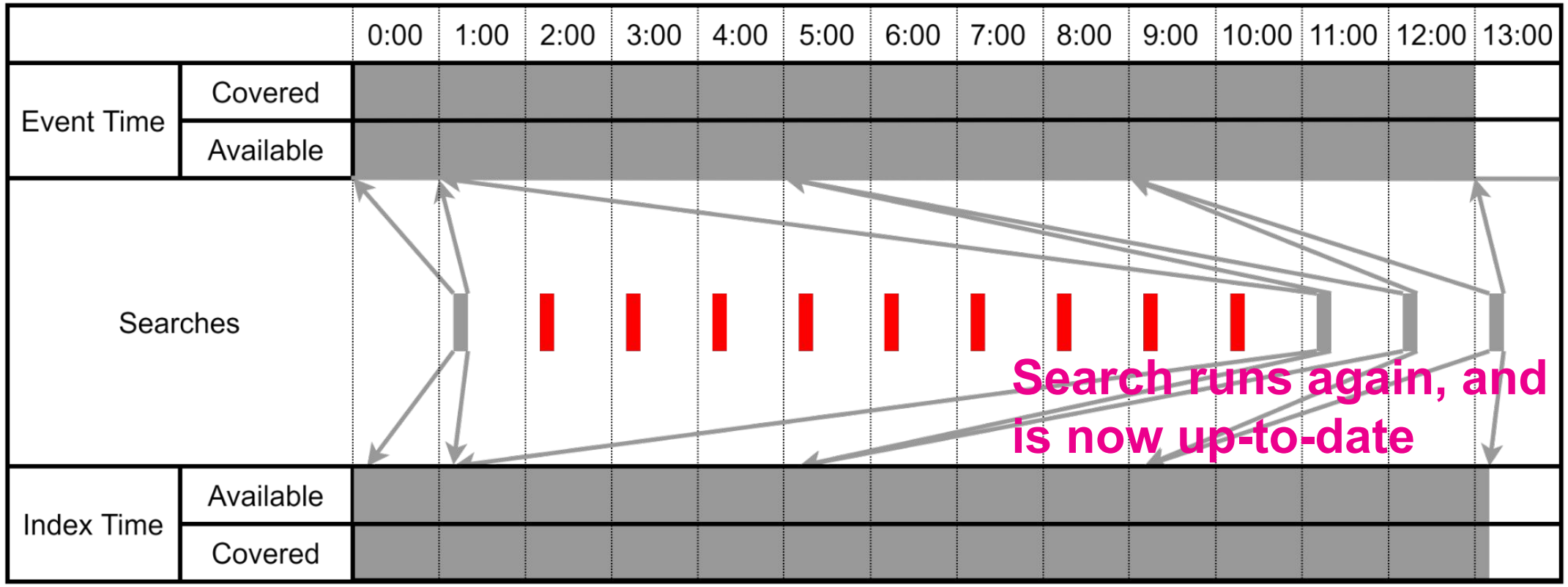
Time: 12:10 **Last Run: 09:10**

Skipped Search / SH Down / Issues | Macro Method



Time: 13:10 **Last Run: 09:10**

Skipped Search / SH Down / Issues | Macro Method



Time: 13:10 **Last Run: 13:10**

Limitations

1) Some searches need event time
   - Comparisons of counts per hour
2) Sub-searches / Multi-searches
3) Mid-search failures (failure after time already updated)
   - Memory hits a limit
   - Disk space runs out
4) Search dependencies
   - Search A generates a lookup used by search B

Advanced Use Cases with Apache Airflow

Apache Airflow is a free and open source platform created to programmatically author, schedule and monitor workflows

Airflow does not interact with Splunk out of the box

Our design:

- Commands Splunk over rest
- Can test if data is present before running a query (Limitation 1)
- Passes in time range to searches either as event or index time (Limitation 2)
- Monitors for completion / success and can parse search.log (Limitation 3)
- Can pull back results
- Uses Airflow's built-in dependency management (Limitation 4)

“So How do I Get Started?”

1

Start using a combination of earliest index time and a sliding scale

```
_index_earliest=-12h@h _index_latest=-0h@h
```

2

Stateful earliest _index_time

- Create KV Store
- Leverage/Adapt provided Macro
- Incorporate Macro in alerts
- Test, Test, Test

3

Apache Airflow

In Conclusion...

- There are real challenges with alerts you want to always run and never miss data
- Different environments are at different places along the journey
- With minimal effort (15 lines of SPL!) you can resolve almost all these challenges
- We showed you how to get started, go explore how you can improve and mature your approach to these challenges

Thank You

Please provide feedback via the

SESSION SURVEY

splunk> .conf21