Complying with the Markets in Financial Instruments Directive II

MiFID and MiFID II are regulations for electronic trading in EMEA. Best execution is a key principle of these directives and states that “take all sufficient steps to obtain, when executing orders, the best possible result for their clients taking into account price, costs, speed, likelihood of execution and settlement, size, nature or any other consideration relevant to the execution of the order.” One standard for adhering to best execution requires firms to show that servers all have time settings that vary no more than one MS from UTC. Another standard requires firms to execute trades at the best possible price among exchanges. Financial markets must adhere to the regulations set forth in these directives to protect investors. There are many searches you can run to help ensure compliance and identify any violations so they can be investigated and prevented in the future.

Required data

- Data:
  - Simple network time protocol logs
  - Business service data for buy and sell orders
- CSV or KV lookup files for
  - NTP data by host
  - Buy or sell order transaction data
  - Reference data that has the price of tradable commodities

How to use Splunk software for this use case

Some commands, parameters, and field names in the searches below may need to be adjusted to match your environment. In addition, to optimize the searches shown below, you should specify an index and a time range when appropriate.

Splunk recommends that customers look into using data models, report acceleration, or summary indexing when searching across hundreds of GBs of events in a single search. The searches provided here are a good starting point, but depending on your data, search time range, and other factors, more can be done to ensure that they scale appropriately.

MiFID II time drift

The MiFID II best execution principle states that firms must “take all sufficient steps to obtain, when executing orders, the best possible result for their clients taking into account price, costs, speed, likelihood of execution and settlement,
size, nature or any other consideration relevant to the execution of the order." Hosts that have a large time drift may effect best execution. You need to monitor for time drift.

Use a script to contact an NTP server on a host every N minutes and capture the results to a file. A script such as echo 'sntp time_server' 'hostname' may be enough.

```bash
|lookup <NTP data by host>
|sort - date
|where drift<-0.1 OR drift>+0.1
```

Need more help with this search? Click here.

---

**MiFID II time drift impact on buy and sell orders**

Hosts that have a large time drift may have business impact on buy and sell orders. You want to see any impacted transactions by listing out the volume and monetary amount that was recorded on that host at the time of intolerable time drifting.

Use a script to contact an NTP server on a host every N minutes and capture the results to a file. A script such as echo 'sntp time_server' 'hostname' may be enough.

```bash
|lookup <NTP data by host>
|sort - date
|where drift<-0.1 OR drift>+0.1
|lookup <transaction data lookup file> host, date
|table date, host, drift, amount, volume
|eval amount=toString(round(amount, 2),"commas")
```

Need more help with this search? Click here.

---

**MiFID II best execution buy and sell violations**

The MiFID II best execution principle states that firms must "take all sufficient steps to obtain, when executing orders, the best possible result for their clients taking into account price, costs, speed, likelihood of execution and settlement, size, nature or any other consideration relevant to the execution of the order." You need to correlate trade logs with pricing databases to see if a trade met best execution for a buyer or if a lower price was found. If the exchange price is lower, it is a violation, and violating best execution may result in penalties.

```bash
|sourcetype=<buy and sell order data source>
|lookup <commodity reference data> _time, symbol OUTPUT exchangeA exchangeB exchangeC
|where (action="buy") AND (amount>exchangeA OR amount>exchangeB OR amount>exchangeC)
```

Need more help with this search? Click here.

---

**Next steps**

The penalties for violating best execution principles of MiFID II can be severe. Schedule these compliance searches to
run and report on a regular basis, investigating as needed and taking appropriate action. For example, if the time drift in the log entry is above a tolerance, the host should be fixed as trades may be impacted. You can also correlate the total volume of trades and monetary amount that was involved for buy or sell orders with hosts experiencing intolerable time drifts. Use this information for your KPIs.

The Splunk Essentials for the Financial Services Industry app helps you automate the searches provided in this article. The app also provides more insight on how they can be applied in your environment, how they work, the difficulty level, and what data can be valuable to run them successfully. In addition, the Splunk Essentials for the Financial Services Industry app provides a number of other compliance solutions for financial services.

Finally, these additional Splunk resources might help you understand and implement this use case:

- .Conf Talk: [40 ways to use Splunk in financial services](#)
- Blog: [MiFID II: The clock is ticking for financial services](#)

---

The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.