# Automation architectures

# CTI?

- IoC / remediation feed

  vs

- intelligence on actors, TTPs, …

# How do you handle information?

~ 5 steps process

1) collect
2) transform
3) store
4) analyze
5) share/apply

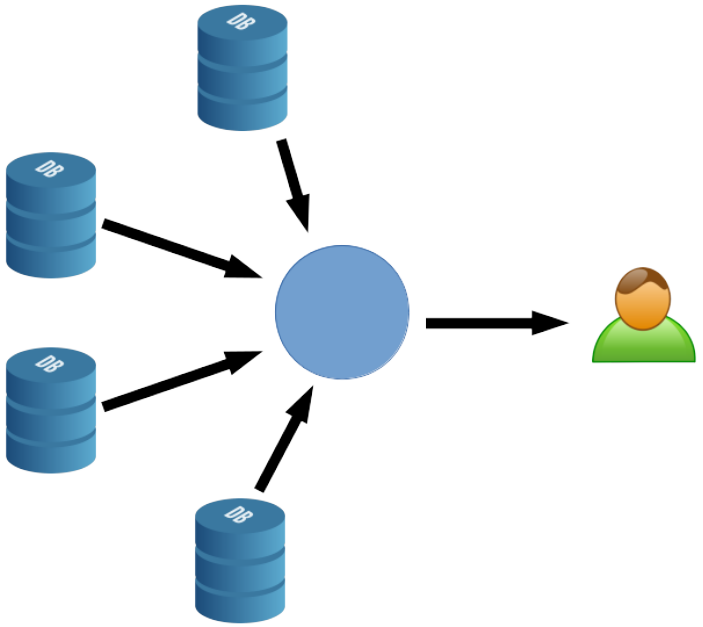
# Automation

- Automate parts of the process
- Efficiency (time saver, delay)
- Enable some activities

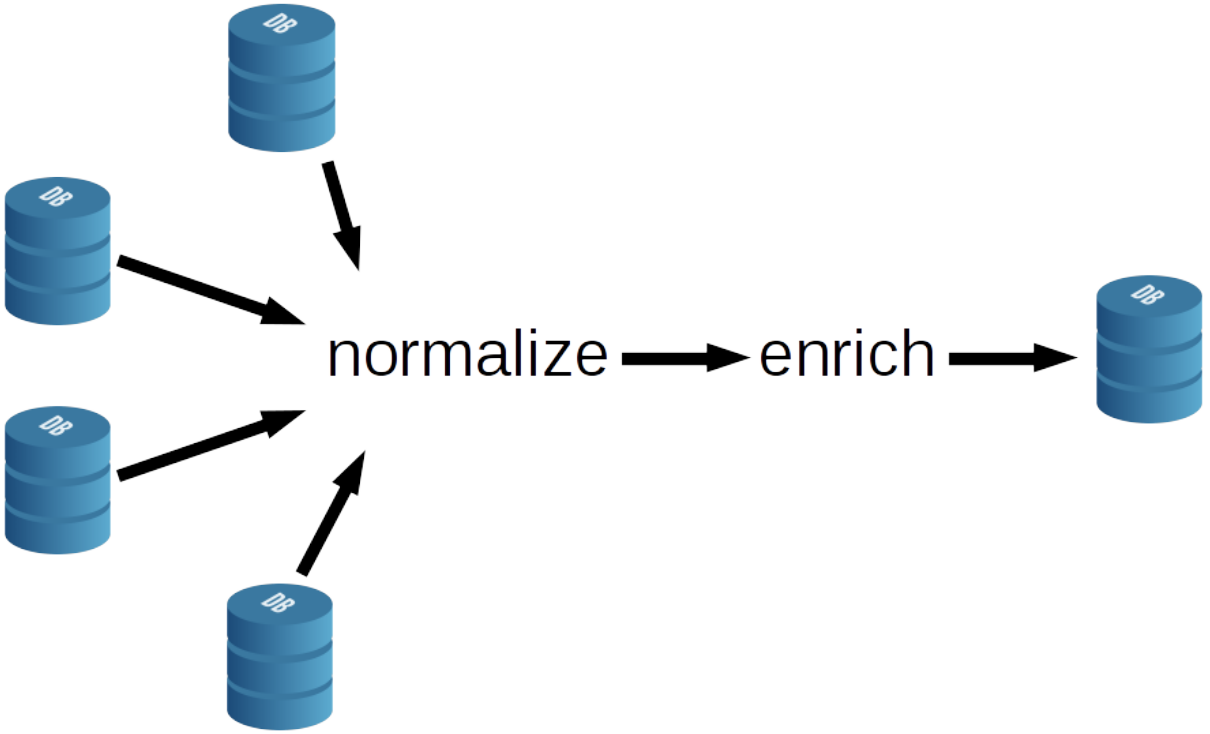
# An idea for this session

- Less focus on tools
- Look at the process
- Identify common patterns
- Share experiences

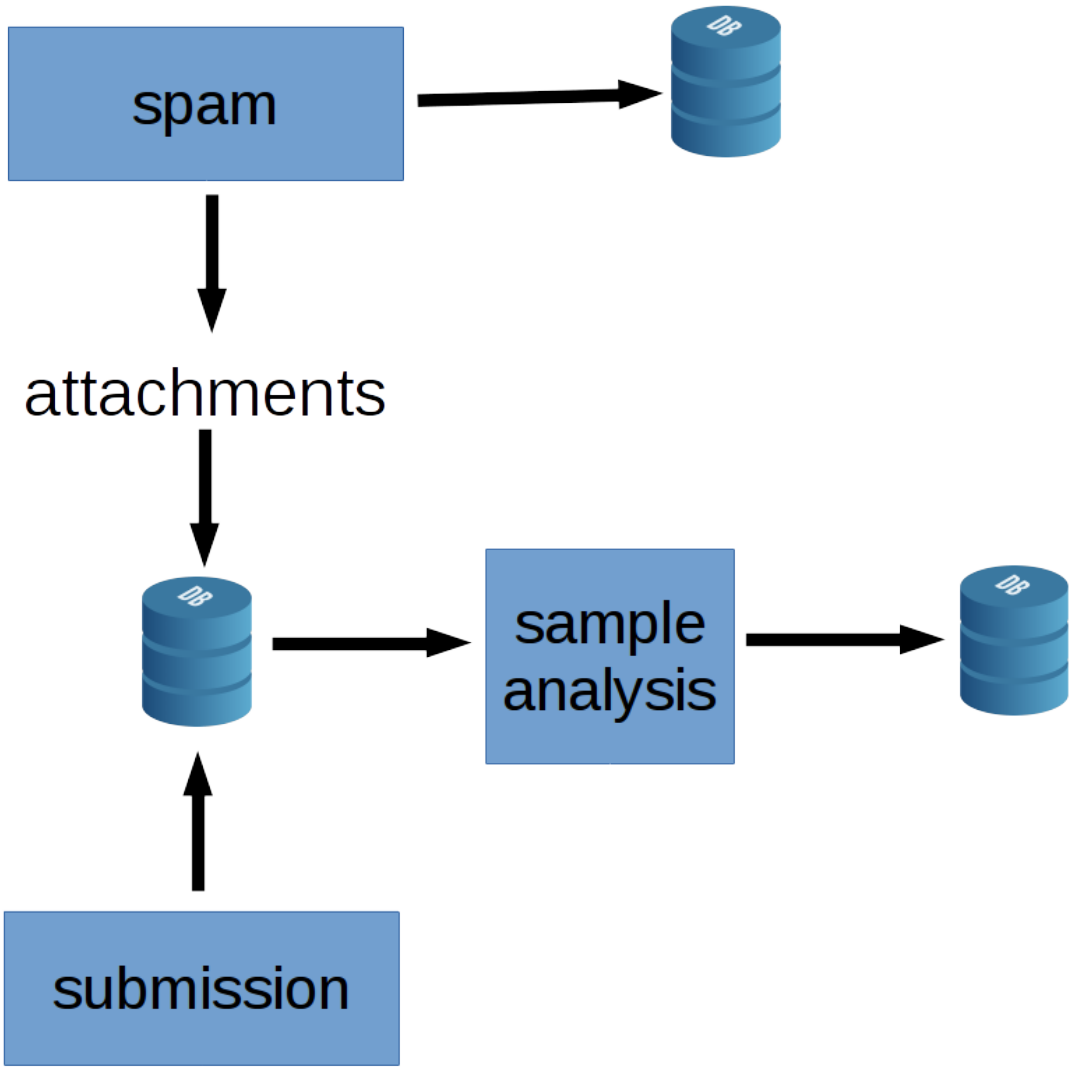
# Basics: centralized query



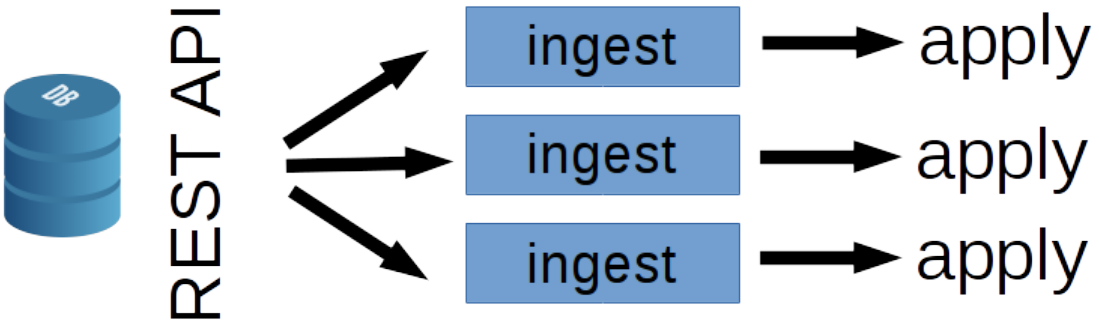
# IntelMQ, n6, Abuse Helper, ...

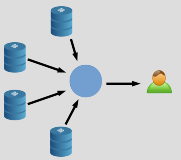
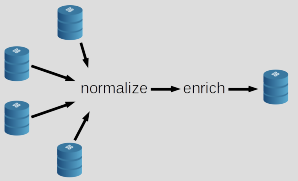


# Malware analysis



# Sharing with constituency
# *(does not work in general)*



| | | Architectures | | |
|---|---|---|---|---|
| | |  |  | ... |
| **Use case / type of information** | IoC feeds | ? | ? | ? |
| | vulnerability reports | ? | ? | ? |
| | threat actor tracking | ? | ? | ? |