What is ECS?

- A specification of common fields and how they should be mapped
- Before ECS, there was no cohesion between field names
- Ingesting logs from nginx would give different field names than Apache 🤯
- ECS means that common fields are named the same thing
    - E.g. `@timestamp`
- Use-case independent
- Groups of fields are referred to as *field sets*

Uses of ECS

- In ECS, documents are referred to as *events*
  - ECS doesn't provide fields for non-events (e.g. products)
- Mostly useful for standard events
  - E.g. web server logs, operating system metrics, etc.
- ECS is automatically handled by Elastic Stack products
  - If you use them, you often won't have to actively deal with ECS
- You might not need to use ECS, but it's good to know what it is 🙂