0.1 Event tracing for Windows

Add proper description of what ETW is.

In the architecture of Event Tracing for Windows (ETW) events are at the centerpiece where they are created, managed and consumed by different event components[1]. These differentiate between event *providers*, event *consumers*, and event *controllers*. All of these event components handle the workflow of ETW, either by reading or writing, or by controlling the events in some way.

0.1.1 Event components

figure out if the components should just be subsections

Controllers

Providers

Providers are the system- and userland applications that provide events and data. They do so by registering themselves as a provider, allowing a controller to enable or disable events. By having the controller control whether events are enabled or not, allows an application to have tracing without generating alerts all the time. This is especially interesting for debugging purposes, which is usually not needed during regular usage.

Many different

Consumers