## 0.1 Event tracing for Windows

Event Tracing for Windows (ETW) is a logging mechanism that is built into the kernel of Windows. It is used by kernel-mode drivers and applications to provide realtime events and tracing features. While ETW is built into most drivers and applications made by Windows, it is also available for developers to use in their own applications. As most privileged applications built into Windows utilize ETW, it is a very good source for telemetry data related to discovering exploit attempts.

In the architecture of ETW events are at the centerpiece where they are created, managed and consumed by different event components[**url:etw:about**]. 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.

Microsoft define four different types of providers depending on the version of Windows and type of application you are interested in.

#### Managed Object Format (MOF) (classic) providers

#### Windows softwarre trace preprocessor (WPP) providers

#### Manifest-based providers

#### TraceLogging providers

#### Consumers

Consumers are applications that consume events from providers. This is done through event *trace sessions*, where one session is created per provider. Consumers have the ability to both receive events in real time from *trace sessions*,

or later on by events stored in log files. Furthermore, events can be filtered by many attributes such as timestamps.

Figure shows how the different components of ETW works together to produce and consume events

add ref to figure

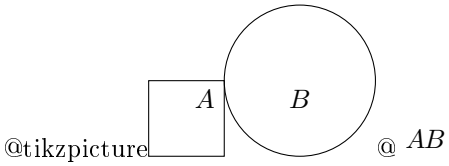


Figure 1: ETW model diagram[**url:etw:about**]

### 0.1.2 Finding providers

### 0.1.3 Consuming events

Mention TI provider and how it is used in many EDRs to detect malicious activity