



WHAT IS EBPf?

Presented by: Ariel Gabay



General Background

eBPF is a technology that allow us to run programs in the kernel, it extends it capabilities dynamically without the need of changing the source code.

This is an event based technology that is widely use for network performance monitoring, security and debugging.



Use Cases & Advantages

- This technology is highly flexible and efficient which uses low overhead thanks to the ability to run within the kernel.
- It is very flexible and secure because it runs in a sandbox which makes it much safer.
- eBPF is mainly used to optimize packet filtering and load balancing.
- Used in intrusion detection systems to lower security threats.

Thanks!