



Contribution ID: 306

Type: **not specified**

## Troubles and Tidbits from Datadog's eBPF journey

*Tuesday, 14 November 2023 15:30 (30 minutes)*

Datadog has been using eBPF in production for observability, security and networking for several years now. While we managed to leverage eBPF to build new features, which would have been impossible otherwise, we also learned a lot the hard way. In this talk, we aim to get into the details of some gotchas, pitfalls and bugs uncovered over the years. You'll learn about eBPF hook points coverage whoopsies, common bypasses for eBPF-based security tools and a couple of unfortunate series of events from Datadog's cloud workload security product. You will also hear about some challenges with using eBPF for networking like using LRU maps at scale, problems with using shared skb mark value and some fun interactions between `sk_reuseport` and `bpf_sk_assign`.

**Primary authors:** FOURNIER, Guillaume (Datadog); MALLA, Hemanth (Datadog)

**Presenters:** FOURNIER, Guillaume (Datadog); MALLA, Hemanth (Datadog)

**Session Classification:** eBPF & Networking

**Track Classification:** eBPF & Networking Track