

What's new?

- Intrusion detection based on syscalls *isn't* — plenty of people have done that
- However, generally, that's vulnerable to attacks against the agent
- So, develop a version that gathers data using vprobes