Contribution ID: **11** Type: **not specified**

Using the OWASP Top 10 to Save the Astronauts from HAL

A discussion of the OWASP ML Top 10 and OWASP LLM Top 10, and how a failure to apply these principles in 2001 A Space Odyssey, led to implementation flaws in HAL 9000, resulting in disastrous consequences for the crew.
There will be a discussion of failures to consider different aspects of both the LLM and ML top 10 during HAL's design and training phases, and the subsequent attempts to implement fixes during the mission. Each omission or failure to apply an OWASP principle, that led to the vulnerabilities will be discussed in detail, and also related to real life applications, to ensure the talk isn't just a geeky discussion of a cool-looking scf-fi AI.

Length

60 minutes

Optional: Speaker / convener biography

Nick Dunn is a former secure software developer, turned penetration tester and an occasional developer of hacking tools and scripts. His work and interests include tool development, code security review, machine learning and secure software development practices.

Primary author: DUNN, Nick

Track Classification: Talks and presentations