SWEETENING CYBERSECURITY WITH ADVANCED ARTIFICIAL INTELLIGENCE.

Background

Researchers at CSIRO's Data61 are developing artificial intelligence (AI) models to automate the creation of honeyfiles, cybersecurity assets camouflaged as sensitive data. These files serve as digital baits, alerting security teams to unauthorised interactions and bolstering network defences against cyberattacks.

Their research requires extensive data manipulation and substantial computational power to train complex generative models.

Challenges

Data61's existing high performance computing (HPC) infrastructure was taking weeks to run a single experiment, impeding the iterative improvement process crucial for developing competitive models.

Data61 required a robust, expertly-supported HPC infrastructure capable of rapidly testing a wide range of sophisticated models.

Solutions

Our HPC Experts ensured a smooth transition to DUG HPC Cloud.

Our tailored support and powerful, bare-metal compute, which includes 80GB NVIDIA A100 GPUs, delivered accelerated data processing and networking capabilities—enabling Data61 to run on-demand experiments in parallel.

Results

Our bespoke HPC solution reduced training times from weeks to 1–2 days, providing Data61 with the time and resources to explore previously inaccessible research areas such as large language models, while also allowing timely publication of results.

With expertly supported access to the latest hardware, the researchers were able to scale their models, benchmark their performance against state-of-the-art approaches, and incorporate larger, more challenging datasets, all helping Data61 to unlock the cybersecurity potential of honeyfiles and push the boundaries of AI capability.