TITLE (20 words maximum)

Turning the tables on cyber attackers, Active Defence at USQ. (Not just F$%#@ honeypots)

ABSTRACT CONTENT (300 words)

The world of a cyber-defender is analogous to asymmetric warfare. Defenders need to “get it right” 100% of the time. Attackers - particularly those who are motivated and patient - only need to get it right 1% to still win. It’s just not fair.

The stakes are getting higher through the increased activity of skilled and motivated attackers and evolving threats such as ransomware which are having weekly impacts across all industries.

This presentation covers USQ’s utilisation of active defence (deception technologies) to provide an edge in detection and defence of systems, endpoints and data. USQ’s practical application of these controls will also be mapped against MITRE Shield for context.

We will cover off the project goals and previous control capability gaps. Subject matter expert Vlado Vajdic from Attivo Networks will also join us for a walkthrough of the technical implementation which includes: Active Directory obfuscation, attack modelling, data cloaking, decoy and breadcrumb deployment, management and SIEM integration.

Future deployment considerations will be discussed including SOAR integration to further enhance adversary engagement and response in real time.

Takeaways:

- Business case for Active Defence
- Terminology & Deployment considerations and integrations
- Active Defence is not just F$%#@ honeypots!

Note due to the sensitive nature of this presentation it will be in person only.