In order to meaningfully manage cyber security risk, remediation activities should be guided by an understanding of how an attacker would realistically target your organisation.

Purple teams are end-to-end attack simulations, which replicate the actions an attacker would take, including technical validation. Collaboration using interviews with your employees is also leveraged, in order to mimic attacker enumeration activities in a time-efficient and cost-effective manner.

The end-to-end nature of a purple team involves mapping out attack paths from a starting point to an end objective associated with meaningful business risks. To replicate real-world attacks, starting positions typically involve the “assumed compromise” of a user through phishing or the compromise of a third party supplier. End objectives typically involve gaining access from the corporate environment to the Operational Technology (OT) environment, and obtaining the capability to influence process control.

**Key Benefits**

- Discovered attack paths relate to realistic threat scenarios
- Recommended security controls provide tangible risk reduction
- Collaboration provides bidirectional knowledge transfer and facilitates remedial actions

**Deliverables**

Applied Risk will provide a detailed technical report including:

- An overview of the findings at an executive level
- Attack path visualisations, at both an executive and technical level
- A detailed attack narrative of identified attack paths
- Recommendations for security controls for prevention, detection, and response