Mitre Att&k Framework in Student CERT

TLP: White

Andrew Roberts

Mitre Att&k is a valuable resource for students and young professionals with interdisciplinary skills to learn and gain knowledge of cyber operations.

Why Student CERT

- Limited CERT resources in small country. Build capability with MSc Program.
- Opportunity for students to learn and be engaged in real-life CERT Operations
- Students partake in role as CERT analyst

How do we train CERT Analysts with no/little experience?

- Legal, Human/Psychological and Management Education
- Table-Top exercising and Rehearsal of Concept for Incident Handling
- Technical training on Monitoring Technologies
- Training for situational awareness understanding construction of cyber attacks using Mitre Att&k Framework

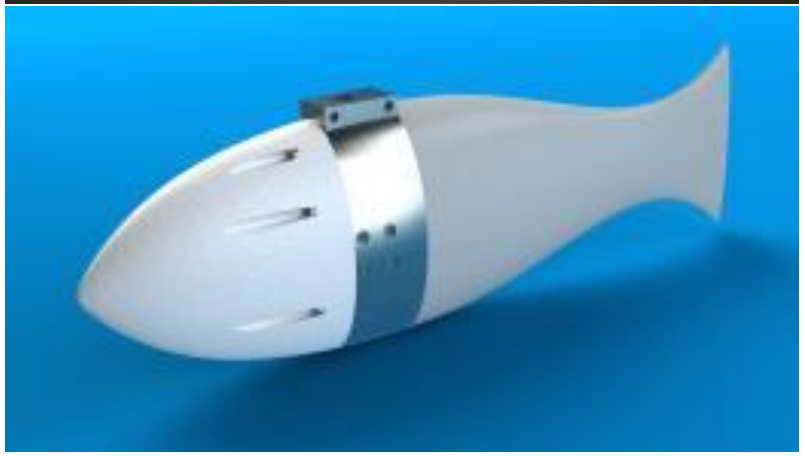
Benefits of Mitre Att&k and Student CERT

- Behavioural Based Model is consumable for students in an interdisciplinary course.
- Mitre Adversary Emulation Plans provide opportunity for students to transform technical skills to understand the operational aspects.
- Learn the complexities and required effort to provide meaningful threat intelligence

Challenges

- Large catalogue of TTPs – not always easy to ingest
- How does Automation of offensive technologies with minimal human interaction affect a behavioural based model?
- Attribution is difficult

Future of Universities



Campus-of-Things

TAL TECH