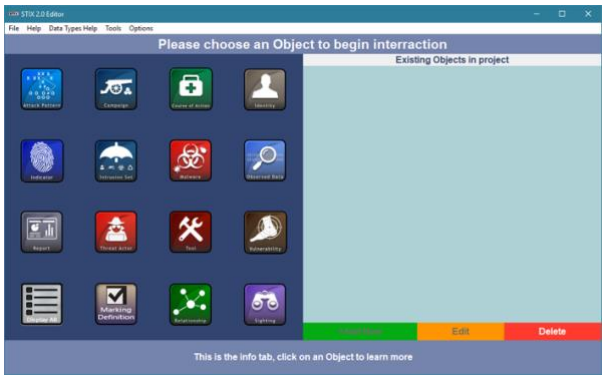
UoM MSN Lab has implemented and tested through several case studies a graphical Cyber Threat Intelligence Editor (the editor is based on the Stix 2.0 language and serialization format and coded on python 3.x taking advantage of multiple open source libraries). The editor aims at providing a friendly platform for users to produce high quality Threat Information Intelligence in a structured manner without any limitations. Through the creation of Stix Bundles, describing and sharing threats of any complexity can be achieved in a very efficient way. Users can create relationships and connections between a plethora of objects available to best describe cyber threats of any scale and as seen fit by the user. The editor can also parse information from Stix files and present them to the user in the most humanly readable way possible for easy edits and additions.



Moreover, the editor is coded in such way that it is very easy to expand and improve it. This also futureproofs the software itself from becoming obsolete in case of future Stix Language changes and upgrades

Easy to use and embedded bug report system for fast and efficient betterment of the application by the developers

By using a friendly and highly customizable graphical user interface it is very easy for users to quickly learn how to use the editor even without prior experience with similar software. The editor is built around innovative ideas both visually and structurally, its most prominent ones being:

- *Built-in documentation segments and dynamic parameter explanations through the GUI interface for fast user adaptation*
- *Backwards compatibility with older Stix versions, Input/Export manipulation freedom*
- *Open and easily parsed by the user filesystem backend*
- *Non-aggressive user input syntax checking and versatile interaction methods*
- *Use of Json data-interchange format for threat information storing and sharing*