Abstract

The number of cyber attacks over the last decade has been increasing sharply while being more and more targeted and sophisticated at the same time. These types of targeted and sophisticated attacks are called advanced persistent threats (APTs) and cause lots of damages to companies through data losses, injecting viruses, amongst others. While cyber threat intelligence has been recognized by experts as an efficient tool to combat APTs, its implementation has been rather slow mainly due to a lack in clarity, consensus, and little academic research as to what exactly is cyber threat intelligence from the perspective of enterprise cyber security. Therefore, there is need to provide a unifying definition of cyber threat intelligence and its creation process from enterprise perspective.

Through the lens of comparative analysis, this paper aims to challenge the stability of currently existing cyber threat intelligence cycles and definitions by a thematic analysis of various cyber security white papers and academic literature. Qualitative analysis will equally permit to have an insider view of the field and forge subjective opinions and allow for ambiguity, contradiction, and the generation of new ideas.