ABSTRACT

In questo lavoro sono stati analizzati il ciclo di Intelligence, le fonti di Intelligence, gli standard di trasmissione e classificazione e gli algoritmi di Intelligenza Artificiale, risultando tutto strettamente collegato. È possibile dunque pensare alla creazione di un sistema basato su Intelligenza Artificiale che sia "addestrato" per la raccolta di un determinato tipo di dato, da una determinata fonte, che si occupi della sua analisi, della creazione di un dato contenente intelligence e della sua disseminazione.

Il processo di intelligence in materia di Cyber Security è molto complesso perché deve tener conto di numerosi "stimoli" forniti dall'ambiente e cercare di prendere in considerazione solo quelli utili, per non sovraccaricare il sistema. La Cyber Threat Intelligence (CTI) deve essere adattata ad ogni singola azienda per essere utile, ma ad oggi il prodotto deve essere vagliato da un essere umano per poter prendere le appropriate decisioni nei momenti critici. La CTI migliore è considerata quella che aiuta un esperto di sicurezza nel processo decisionale, che gli dà un valore aggiunto nel prendere decisioni corrette, appropriate e soprattutto in tempi sufficientemente brevi da evitare l'intrusione su vasta scala o un'interruzione dei servizi.

L'innovazione offerta dalla CTI non è quella di saper riconoscere un attacco noto, ma riconoscere le azioni subdole che vengono effettuate su un sistema che si conosce. Questo processo è possibile attraverso l'analisi in tempo reale delle anomalie che risultano ricche di informazione in quanto vengono correlate con molteplici indicatori che presi singolarmente risultano invece molto deboli.

La CTI deve guidare nel prendere decisioni e produrre informazione quando le infiltrazioni sono nella loro fase iniziale e gestibile, in una finestra temporale che consenta di verificarne l'efficacia ed evitare che la situazione diventi critica. In questo contesto può essere molto utile un approccio attraverso le Reti Neurali, che assicurano un livello di accuratezza elevato e soprattutto rendono le operazioni più snelle e veloci. Sicuramente siamo molto lontani dall'avere un sistema completamente automatizzato, ma si può pensare all'integrazione di vari sistemi come ad esempio Reti Neurali per snellire il processo, Sistemi Esperti per diminuire i falsi positivi e analisi dell'informazione creata da parte degli esperti aziendali di sicurezza per prendere le decisioni definitive.