Esercitazione WEEK 19 D1 (2)

Threat Intelligence

Ettore Farris

Descrizione sintetica

Quanti e quali sono i livelli su cui è basato il sistema di valutazione di ThreatConnect? Compila una lista spiegando, per ogni livello, le caratteristiche.

Soluzione

Un modo per valutare la qualità delle informazioni ottenute mediante un'operazione di Threat Intelligence è verificare il *confidence factor,* ovvero il fattore di fiducia. Più alto è il confidence factor e più le informazioni sono rilevanti. Tuttavia, le informazioni con un basso indice non andrebbero scartate in quanto potrebbero essere confermate in seguito.

ThreatConnect utilizza il seguente sistema di valutazione delle informazioni in una scala da 1 a 100:

- **Confermata (90-100):** l'informazione è confermata da fonti autorevoli;
- **Probabile (70-89):** la minaccia non è stata ancora confermata, ma ci sono segnali che ne suggeriscono l'attendibilità;
- **Possibile (50-69):** alcune delle informazioni indicano un grado di veridicità concreto, ma non ci sono ancora evidenze per confermare la minaccia;
- **Incerta (30-49):** la valutazione dell'informazione è possibile, ma sono necessarie più informazioni per identificare la minaccia
- **Improbabile (2-29):** la valutazione dell'informazione è possibile, ma non è la scelta più logica, data la presenza di informazioni discordanti
- **Screditata (1):** esiste la conferma che la minaccia non è reale.