INDICATOR THREAT AND CONFIDENCE RATINGS

W19D1

CONFERMATA (CONFIRMED, 90–100)

- Informazione confermata da più fonti o da analisi diretta; la minaccia risulta **reale.**

applicazione pratica

- Usare l'informazione per prendere decisioni rapide a livello direzionale e attivare azioni di contenimento

PROBABILE (PROBABLE, 70–89)

- Non ancora confermata, ma **coerente e plausibile**; molti segnali indicano un'**alta probabilità** che la minaccia sia reale.

Applicazione pratica

- Monitoraggio attivo e preparazione di piani di risposta preventivi.

POSSIBILE (POSSIBLE, 50–69)

- Alcune informazioni indicano **veridicità concreta**, ma **mancano evidenze** per confermare la minaccia.

Applicazione pratica

- Investigazione approfondita e raccolta di ulteriori intelligence, eseguire analisi **forense** e **threat hunting** per validare o smentire l'ipotesi di minaccia

INCERTA (DOUBTFUL, 30–49)

- Valutazione **possibile ma non suffragata**; servono **ulteriori elementi** per identificare la minaccia.

Applicazione pratica

- Fase di raccolta dati preliminare con cautela nell'implementazione di misure. Limitarsi a raccolta e normalizzazione dei dati a piccole misure a basso impatto evitando blocchi aggressivi finché non arrivano conferme.

IMPROBABILE (IMPROBABLE, 2–29)

- Possibile ma poco logica e contraddetta da altre informazioni.

Applicazione pratica

- Monitoraggio passivo senza allocazione significativa di risorse. Tenere l'argomento **sotto osservazione** attraverso dashboard e alert a **bassa priorità.**

SCREDITATA (DISCREDITED, 1)

- La valutazione ha confermato che la minaccia **non è reale**.

Applicazione pratica

- Procedere alla declassificazione/chiusura