

Livelli di Affidabilità delle Valutazioni di Sicurezza

Certamente Affidabile (90-100)

- **Descrizione:** La valutazione è confermata da fonti indipendenti o attraverso un'analisi diretta e approfondita. Non ci sono dubbi sulla sua correttezza. L'interpretazione è logica e completamente coerente con altre prove o informazioni sull'argomento.
 - **Esempio:**
 - *"Questo file eseguibile distribuisce con assoluta certezza una variante nota di malware."*
-

Molto Probabile (70-89)

- **Descrizione:** La valutazione non è verificata in modo diretto, ma è altamente ragionevole e si allinea perfettamente con altre informazioni disponibili. Anche se non è confermata al 100%, ci sono buoni motivi per ritenerla corretta.
 - **Esempio:**
 - *"L'URL presenta una struttura simile a quella di altri URL riconosciuti come malevoli, anche se appartiene a un host diverso."*
-

Probabile ma non Sicuro (50-69)

- **Descrizione:** La valutazione ha una logica di fondo, ma non tutte le informazioni sono in pieno accordo. C'è una certa probabilità che sia corretta, ma è necessario ulteriore approfondimento per avere conferme definitive.
 - **Esempio:**
 - *"L'indirizzo email coincide con il nome utente trovato durante l'analisi del malware, ma potrebbe trattarsi di una coincidenza data la sua comunanza."*
-

Incerto e Non Corroborato (30-49)

- **Descrizione:** La valutazione potrebbe essere plausibile, ma non rappresenta la spiegazione più logica. Non ci sono informazioni sufficienti a confermare né a smentire completamente la valutazione, e potrebbe trattarsi di un falso positivo.
 - **Esempio:**
 - *"Le scansioni provengono da un indirizzo IP fornito da un provider VPS, ma non ci sono prove sufficienti per stabilire con certezza se sia dannoso."*
-

Improbabile e Contraddetto (2-29)

- **Descrizione:** La valutazione, sebbene tecnicamente possibile, non rappresenta la conclusione più razionale. Al contrario, è in conflitto con altre informazioni più attendibili e ha poche probabilità di essere corretta.
 - **Esempio:**
 - *"Il file si connette a un host che sembra essere stato disabilitato. È improbabile che sia attualmente in uso come comando e controllo (C2)."*
-

Smentito (1)

- **Descrizione:** La valutazione è stata dimostrata chiaramente errata, basata su prove che la confutano. Non c'è più alcun dubbio riguardo la sua inesattezza.
 - **Esempio:**
 - *"Questa non è una minaccia malware; si tratta solo di una banale presentazione PowerPoint® mal formattata."*
-

Non Valutato (0)

- **Descrizione:** Nessuna analisi è stata effettuata sull'indicatore o non è stata assegnata alcuna valutazione in termini di affidabilità. Questo livello indica un'incertezza completa, dove mancano informazioni o prove.
-

Conclusione

Questi livelli di affidabilità rappresentano una scala utile per valutare la sicurezza e l'accuratezza delle informazioni. Dalla certezza assoluta fino all'assenza di valutazione, questo sistema aiuta a gestire i rischi e a prendere decisioni informate in scenari di cybersecurity e analisi di dati.