INDICATOR THREAT AND CONFIDENCE RATINGS

W19D1

LIVELLI DI CONFIDENCE RATING

CONFERMATA (Confirmed, 90–100)

L’informazione è stata verificata da più fonti attendibili o da analisi diretta: la minaccia è reale e attuale.

Applicazione pratica: usare immediatamente l’informazione per decisioni a livello direzionale e attivare azioni di contenimento (isolamento host, blocco accessi, aggiornamento regole di sicurezza).

Esempio: "Lo stesso dominio di C2 è confermato dai nostri log, da un sandbox esterno e da un report del vendor: trattiamolo come compromissione certa."

PROBABILE (Probable, 70–89)

L’informazione non è ancora pienamente confermata, ma è coerente, plausibile e supportata da diversi segnali convergenti: è molto probabile che la minaccia sia reale.

Applicazione pratica: attivare monitoraggio attivo, innalzare il livello di allerta e predisporre piani di risposta e contenimento pronti all’uso.

Esempio: "Più host interrogano lo stesso dominio sospetto dopo una campagna di phishing mirata: non è provato al 100%, ma ci prepariamo a bloccarlo e a isolare le macchine coinvolte."

POSSIBILE (Possible, 50–69)

Esistono elementi concreti che indicano una potenziale minaccia, ma le evidenze sono incomplete e non permettono di confermare o smentire con certezza.

Applicazione pratica: condurre investigazioni approfondite, raccogliere ulteriore intelligence, avviare analisi forense mirata e attività di threat hunting per validare o smentire l’ipotesi.

Esempio: "Abbiamo trovato un eseguibile sospetto su un singolo endpoint, ma senza traffico anomalo associato: avviamo analisi forense e hunting su file simili nel resto dell’ambiente."

INCERTA (Doubtful, 30–49)

La valutazione è teoricamente possibile ma poco supportata; mancano dati solidi e il quadro è troppo vago per identificare con chiarezza la minaccia.

Applicazione pratica: restare in fase di raccolta dati preliminare, con misure caute e a basso impatto. Limitarsi a logging, normalizzazione dei dati e piccoli aggiustamenti non invasivi, evitando blocchi aggressivi finché non arrivano conferme.

Esempio: "Un unico alert generico da un vecchio IDS segnala attività sospetta, ma senza altri indizi: aumentiamo la visibilità e affiniamo le regole, senza bloccare nulla in produzione."

IMPROBABILE (Improbable, 2–29)

La minaccia è teoricamente possibile, ma appare poco logica, scarsamente plausibile o contraddetta da altre informazioni più solide.

Applicazione pratica: mantenere solo un monitoraggio passivo, senza dedicare risorse significative. Tenere l'argomento sotto osservazione tramite dashboard e alert a bassa priorità.

Esempio: "Un solo IP esterno, catalogato come benigno da più fonti, è segnalato come malevolo da una lista poco affidabile: lo teniamo d'occhio ma non modifichiamo le policy."

SCREDITATA (Discredited, 1)

Le analisi hanno dimostrato che la minaccia non è reale o che l'informazione di partenza era errata o fuorviante.

Applicazione pratica: procedere alla declassificazione o chiusura del caso, aggiornando la documentazione e, se necessario, correggendo le regole o le fonti che hanno generato il falso allarme.

Esempio: "Il dominio segnalato come malevolo risulta essere un servizio interno legittimo mal etichettato: chiudiamo l'incidente e aggiorniamo le whitelist."

LIVELLI DI THREAT RATING

0 (Unknown - Sconosciuto)

Non disponiamo di dati sufficienti o attendibili per classificare il livello di minaccia.
Esempio: "Ho solo un paio di log parziali, non posso ancora dire se ci sia qualcosa di sospetto o no."

---

1 (Suspicious - Sospetto)

Non è stata ancora identificata attività chiaramente malevola, ma ci sono segnali anomali o comportamenti fuori norma che meritano indagine.
Esempio: "Questi accessi fuori orario da un nuovo IP non sono necessariamente malevoli, ma non sono neanche normali per il nostro ambiente."

---

2 (Low Threat - Minaccia Bassa)

Indica un avversario poco sofisticato o attività automatizzata e opportunistica, spesso riconducibile a scansioni o tentativi generici di ricognizione iniziale.
Esempio: "Vediamo tentativi di login con password comuni da varie IP listate in blacklist pubbliche, ma nessuno sembra andare a buon fine."

---

3 (Moderate Threat - Minaccia Moderata)

Indica un avversario con discrete capacità tecniche e un obiettivo definito; l'attività osservata è coerente con fasi centrali della kill chain (consegna, exploit, installazione).
Esempio: "Quell'attachment PDF contiene uno sfruttamento mirato a una specifica versione del nostro software contabile usato solo dall'ufficio finanza."

---

4 (High Threat - Minaccia Alta)

Rimanda a un avversario avanzato che ha già condotto azioni mirate e persistenti nell'ambiente, con indizi di compromissione in corso o già avvenuta.
Esempio: "Troviamo lo stesso dominio di C2 su più host interni e persistenza configurata su almeno tre server critici."

---

5 (Critical Threat - Minaccia Critica)

Rappresenta un avversario estremamente competente, ben finanziato e già in grado di impattare direttamente la confidenzialità, integrità o disponibilità di asset critici. Richiede risposta immediata ed estrema.
Esempio: "Le chiavi di cifratura del database clienti sono state esfiltrate e vediamo manipolazioni in tempo reale dei dati di produzione."