Team 1

Epicode

Threat Intelligence

W19D1 - 21 gennaio 2025

Indice

.

Introduzione

Il sistema di valutazione di **ThreatConnect** si basa su due scale principali: **Threat Rating** (valutazione della minaccia) e **Confidence Rating** (valutazione della fiducia). Ogni scala è suddivisa in livelli, ognuno con specifiche caratteristiche e criteri di applicazione. Di seguito, vengono descritti i livelli e le loro caratteristiche secondo le best practice indicate da ThreatConnect.

1. Threat Rating (Valutazione della Minaccia)

La **Threat Rating** misura la gravità di una minaccia su una scala da **0 a 5 skulls** (teschi). Questa scala valuta la pericolosità e la fase di avanzamento dell'attacco associato a un indicatore.

Livelli:

1. **Unknown (0 skulls)**:

Caratteristiche: Non ci sono informazioni sufficienti per valutare la minaccia.

Esempio: Analisi preliminare di un’email senza dati sufficienti sul server SMTP.

Fase: Non classificabile.

2. **Suspicious (1 skull):**

Caratteristiche: Non è stata confermata attività dannosa, ma si osservano comportamenti sospetti.

Esempio: Attività insolita verso un URL senza prove evidenti di malevolenza.

Fase: Indizi iniziali di possibile minaccia.

3. **Low Threat (2 skulls):**

Caratteristiche: Avversario opportunistico e poco sofisticato; attività pre-attacco.

Esempio: Scansioni di rete o tentativi di connessione non riusciti.

Fase: Potenziale preparazione per un attacco più significativo.

4. **Moderate Threat (3 skulls):**

Caratteristiche: Avversario con competenze e risorse di base; attività mirata ma non persistente.

Esempio: File dannosi che tentano di sfruttare una vulnerabilità specifica.

Fase: Intrusione attiva (es., delivery, exploitation o installazione).

5. **High Threat (4 skulls):**

Caratteristiche: Avversario avanzato con risorse significative; attività persistente e mirata.

Esempio: Comandi e controlli (C2) osservati durante un'intrusione mirata.

Fase: Post-compromissione (es., movimento laterale o esfiltrazione dati).

6. **Critical Threat (5 skulls):**

Caratteristiche: Avversario altamente sofisticato e ben finanziato; attività devastante in qualsiasi fase.

Esempio: Esfiltrazione dati sensibili attraverso un host intermedio.

Fase: Qualsiasi fase della kill chain.

2. Confidence Rating (Valutazione della Fiducia)

La **Confidence Rating** misura il grado di certezza nella valutazione di una minaccia, su una scala da **0 a 100**. Considera la validità e l'affidabilità delle informazioni raccolte.

Livelli:

1. **Unassessed (0):**

Caratteristiche: Non è stata effettuata alcuna valutazione.

Esempio: Un indicatore raccolto ma non analizzato.

2. **Discredited (1):**

Caratteristiche: La valutazione è stata confutata e si è rivelata errata.

Esempio: Malware classificato erroneamente come file legittimo.

3. **Improbable (2–29):**

Caratteristiche: Le informazioni sono non plausibili o contraddette da altre evidenze.

Esempio: Host sospetto ma già disattivato.

4. **Doubtful (30–49):**

Caratteristiche: Possibile ma non logico; mancano informazioni aggiuntive.

Esempio: Traffico insolito su un indirizzo IP senza ulteriori prove.

5. **Possible (50–69):**

Caratteristiche: Plausibile e coerente con alcune informazioni disponibili.

Esempio: Comportamenti che richiamano schemi di malware noti.

6. **Probable (70–89):**

Caratteristiche: Logico e plausibile; coerente con altre informazioni affidabili.

Esempio: URL che utilizza schemi simili a quelli di minacce confermate.

7. **Confirmed (90–100):**

Caratteristiche: Confermata da fonti indipendenti o analisi diretta.

Esempio: Eseguibile che rilascia varianti di malware note.

Fattori di Valutazione:

- **Conferma:** È stato verificato da fonti affidabili?
- **Plausibilità:** È logico e coerente con i dati disponibili?
- **Coerenza:** Si allinea con altre informazioni affidabili?

Best Practice: Come Utilizzare le Scale

- **Standardizzazione:** Assicurarsi che l'intera organizzazione interpreti i livelli in modo uniforme.
- **Automazione:** Utilizzare processi automatici per "invecchiare" gli indicatori obsoleti e ridurne il Confidence Rating.
- **Risposta:** Impostare azioni basate su combinazioni di **Threat Rating** e **Confidence Rating** (es., blocco automatico di indicatori con Threat Rating di 5 e Confidence superiore a 70).

Conclusione

Il sistema di valutazione di **ThreatConnect** consente di categorizzare indicatori di minaccia in modo efficace, supportando la gestione del rischio e le decisioni aziendali. La combinazione di **Threat Rating** e **Confidence Rating** permette di bilanciare l'urgenza della minaccia con la certezza della sua validità, ottimizzando le risposte di sicurezza.

Facoltativo

Il Rapporto Clusit 2024 evidenzia un aumento significativo degli attacchi informatici, con una crescita del 23% rispetto al semestre precedente, registrando una media di 9 attacchi gravi al giorno a livello globale.

Ecco un elenco delle minacce informatiche più comuni che possono colpire un'azienda:

1. **Malware**: Software dannoso progettato per infiltrarsi, danneggiare o disabilitare sistemi informatici. Include virus, worm, trojan, ransomware e spyware. Ad esempio, nel 2023, il malware ha rappresentato il 36% degli attacchi a livello mondiale.

2. **Phishing**: Tecnica di ingegneria sociale in cui gli aggressori inviano comunicazioni fraudolente, spesso via email, fingendosi enti affidabili per indurre le vittime a rivelare informazioni sensibili. Questa pratica è tra le minacce informatiche più frequenti ed efficaci.

3. **Attacchi DDoS (Distributed Denial of Service)**: Tentativi di rendere un servizio online non disponibile sovraccaricando il server con un traffico massiccio proveniente da più fonti. Questi attacchi possono causare interruzioni significative dei servizi aziendali.

4. **Furto di dati**: Accesso non autorizzato a informazioni sensibili dell'azienda, come dati finanziari o personali, spesso con l'intento di utilizzarli per scopi fraudolenti o di rivenderli nel mercato nero. Questo tipo di minaccia può derivare da attacchi

mirati o da vulnerabilità nei sistemi di sicurezza.

5. **Attacchi alla supply chain**: Compromissione di un'organizzazione attraverso vulnerabilità presenti nei fornitori o partner commerciali. Questi attacchi possono introdurre malware o altre minacce nel sistema aziendale tramite componenti o software di terze parti.

6. **Attacchi "Man-in-the-Middle" (MitM)**: Quando un aggressore si inserisce nelle comunicazioni tra due parti per intercettare, alterare o rubare dati sensibili senza che le vittime se ne accorgano. Questi attacchi possono compromettere la riservatezza e l'integrità delle comunicazioni aziendali.

7. **Attacchi Zero-Day**: Sfruttamento di vulnerabilità sconosciute nei software o hardware, per le quali non esistono ancora patch o soluzioni. Queste minacce sono particolarmente pericolose poiché non rilevabili dai sistemi di sicurezza tradizionali.

8. **Social Engineering**: Manipolazione psicologica delle persone per indurle a compiere azioni o divulgare informazioni riservate. Questo approccio sfrutta la fiducia o l'ignoranza degli individui per ottenere accesso non autorizzato ai sistemi aziendali.

Per proteggersi efficacemente da queste minacce, è fondamentale che le aziende implementino misure di sicurezza adeguate, formino regolarmente il personale sulla consapevolezza delle minacce informatiche e mantengano aggiornati i propri sistemi e software.