M5 D5

ESERCIZIO 2

TRACCIA

THREATCONNECT

ThreatConnect è una piattaforma di gestione delle minacce e intelligence che offre funzionalità di valutazione delle minacce.

Il sistema di valutazione di ThreatConnect si basa su quattro livelli principali:

1) **Livello 1: Individuazione**

   - Questo livello si concentra sull'individuazione delle minacce iniziali.

   - Include indicatori di compromissione (IOC) di base, come indirizzi IP, URL, hash di file e nomi di dominio associati a potenziali minacce.

   Il livello 1 fornisce informazioni essenziali per rilevare e bloccare minacce note.

2) **Livello 2: Conferma**

   - A questo livello, le informazioni raccolte vengono confermate e approfondite per garantire una maggiore precisione.

   - Include l'analisi delle minacce, la correlazione di eventi e l'individuazione di modelli di attacco.

   - Vengono aggiunte informazioni contestuali e dettagliate, consentendo una migliore comprensione delle minacce e delle loro intenzioni.

3) **Livello 3: Analisi**

   - Questo livello comporta un'analisi approfondita delle minacce e dei loro attributi.

   - Include l'analisi dei gruppi di minacce, delle tattiche, delle tecniche e delle procedure (TTP) utilizzate dagli attori delle minacce.

   - Vengono fornite informazioni sulle motivazioni, gli obiettivi e le capacità degli attori delle minacce, consentendo una comprensione più completa del contesto.

4) **Livello 4: Intelligence strategica**

   - Questo è il livello più avanzato e comprende informazioni strategiche sulle minacce.

   - Include analisi approfondite sulle tendenze emergenti, gli scenari futuri e le prospettive delle minacce.

   - Le informazioni di intelligence strategica aiutano a prendere decisioni informate sulla gestione delle minacce, la pianificazione e le strategie di mitigazione a lungo termine.

   Le specifiche di ciascun livello possono variare a seconda della configurazione e delle personalizzazioni della piattaforma ThreatConnect utilizzata dall'organizzazione. Tuttavia, questi sono i livelli di base che compongono il sistema di valutazione delle minacce di ThreatConnect. La valutazione delle minacce è un processo continuo e dinamico. Le informazioni devono essere costantemente aggiornate e analizzate per mantenere la sicurezza dell'organizzazione al passo con le minacce in evoluzione.

TRACCIA 2

TekDefense Automater

TekDefense Automater è uno strumento open-source sviluppato da TekDefense che automatizza il processo di analisi delle minacce informatiche. È progettato per semplificare la raccolta di informazioni e l'analisi dei campioni di file sospetti o delle minacce rilevate.

L'obiettivo principale di TekDefense Automater è quello di automatizzare il processo di ricerca e raccolta di informazioni sulle minacce, riducendo il tempo e lo sforzo necessario per analizzare manualmente i campioni. Può essere utilizzato da analisti di sicurezza, ricercatori di malware e professionisti della sicurezza per ottenere informazioni aggiuntive sui campioni di file o per individuare correlazioni tra diverse minacce.

TekDefense Automater integra diversi strumenti e servizi di intelligence sulla sicurezza, come VirusTotal, Malware Information Sharing Platform (MISP), PassiveTotal, OpenDNS Investigate.

Utilizzando queste fonti, Automater può ottenere informazioni su indicatori di compromissione (IOC), analizzare campioni di file, ottenere informazioni sulle infrastrutture malevoli e fornire una visione più completa di una potenziale minaccia.

Il vantaggio principale di TekDefense Automater è l'automazione del processo, che consente agli utenti di analizzare rapidamente e in modo efficiente grandi quantità di campioni di file o di sospetti. Ciò può fornire una visione più rapida e completa delle minacce e consentire una risposta più tempestiva alle potenziali violazioni di sicurezza.

È importante notare che TekDefense Automater è uno strumento open-source, il che significa che il codice sorgente è accessibile e può essere personalizzato o adattato in base alle esigenze specifiche degli utenti.