Cyber Threat Intelligence

Rileva e classifica le minacce del cyberspazio, aiuta gli operatori IT di un'organizzazione a mitigarne gli effetti

QUALE PROBLEMA RISOLVE QUESTO STRUMENTO?

Lo scopo del tool è rilevare costantemente gli indizi anche più piccoli di rischi informatici per la rete di un'organizzazione sia in forum e compravendite nel deep e dark web, sia in siti di messaggistica.
Senza lo strumento, gli analisti devono manualmente effettuare complesse attività come:

- Raccolta dati relativi a dominio, indirizzi IP e di terze parti.
- Indicizzazione, codifica e analisi dei metadati dei dati raccolti.
- Estrazione dei dati rilevanti, ripristino e predisposizione per l'archiviazione in un database gestito dal fornitore (Cybersixgill).

Con lo strumento si è in grado di:

- Ricevere e utilizzare un elenco di allarmi diversi a seconda del tipo di asset.
- Effettuare indagini offline e circostanziate su minacce presenti o attività in corso nel cyberspazio.
- Ricevere informazioni relative a rischi per l'organizzazione (chi, dove, cosa) e mitigarli.

COME VIENE UTILIZZATO IN IMPETUS?

- **Chi sono gli utilizzatori**: Specialisti IT chiamati ad allertare subito gli operatori delle Centrali Operative o altri attori quali forze di polizia, autorità locali, management, ecc. riguardo a potenziali rischi per gli asset dell'organizzazione.
- **Quali sono le situazioni critiche per il suo utilizzo:** Regolarmente. In genere le scansioni si effettuano quotidianamente. Lo strumento fornisce tutte le informazioni sulla natura e l'origine delle minacce informatiche rilevate. Poiché ne nascono di nuove continuamente, la scansione va replicata

COME FUNZIONA?

I passaggi principali sono:

1. **Data collection:** trovare le fonti rilevanti, accedere a forum e gruppi chiusi e reperire i dati (*crawling*). **Data processing and analysis:** il tool processa ogni elemento raccolto via: *indexing, enrichment, tagging, entity extraction, metadata,* ripristino e salvataggio dati in un database.
2. **Data lake query:** ricerche automatizzate o manuali sono effettuabili sul database del fornitore che conserva ampia casistica di problemi informatici e attività cybercriminali.

This project receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883286