Cyber Threat Detection and Response

Rileva le vulnerabilità informatiche nei sistemi IT: genera allarmi e suggerisce contromisure

QUALE PROBLEMA RISOLVE QUESTO STRUMENTO?

I sistemi informatici presentano in genere così tante vulnerabilità che non è possibile monitorarle continuamente o gestirle tutte manualmente. Inoltre, esistono complesse interdipendenze tra le vulnerabilità. Ad esempio: alcune diventano critiche solo quando un'altra è stata "sfruttata" (come dopo un attacco riuscito). Questo strumento:

- Identifica le vulnerabilità sfruttate e quelle potenzialmente utilizzabili
- Assegna priorità alle azioni per sistemare le vulnerabilità sfruttate e le eventuali vulnerabilità sfruttabili in base alla criticità della situazione

Senza lo strumento:

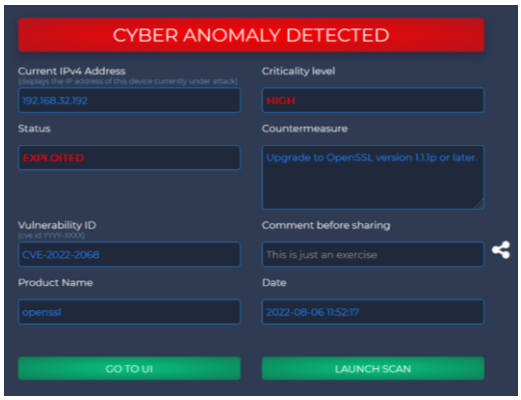
- Le analisi svolte manualmente identificano solo una parte delle vulnerabilità del sistema
- Gli utenti non possono sapere come l'interconnessione tra vulnerabilità può esporre il sistema
- Gli utenti non possono sapere quando una vulnerabilità è stata effettivamente sfruttata

Con lo strumento:

- Gli utenti possono scandagliare sistemi complessi e identificare vulnerabilità e loro connessioni
- Gli utenti possono monitorare i sistemi in tempo reale e ricevere un avviso sulla piattaforma IMPETUS quando una vulnerabilità viene utilizzate.
- Le contromisure possono essere prioritizzate in base alla criticità del rischio

COME VIENE UTILIZZATO IN IMPETUS?

- **Chi sono gli utilizzatori**: (A) specialisti IT responsabili della protezione della rete da possibili attacchi informatici (attraverso analisi, monitoraggio e mitigazione); (B) Sistemisti e operatori delle Centrali Operative centri che vengono allertati in caso di rischi imminenti/situazioni problematiche.
- **Quali sono le situazioni critiche per il suo utilizzo:** Regolarmente: le scansioni e le analisi verrebbero eseguite periodicamente. Lo strumento è progettato per un monitoraggio continuo



COME FUNZIONA?

Analizza i dati in rete e li correla con le vulnerabilità rilevate scansionando l'infrastruttura IT. Quando viene rilevata una minaccia alle vulnerabilità del sistema, le contromisure vengono classificate in base alla gravità del rischio. Viene generato un allarme e inviato alla piattaforma IMPETUS. Gli utenti possono quindi implementare la contromisura. Ad esempio, se un utente tenta più volte di accedere da remoto a una macchina, lo strumento genererà un allarme suggerendo di inibire l'accesso.

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