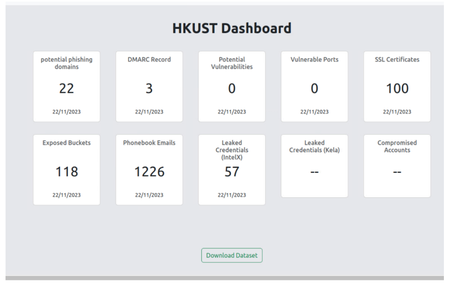
External Cyber Threat Intelligence

Calvin Wiogo
Supervised by Professor Brian Mak

Introduction

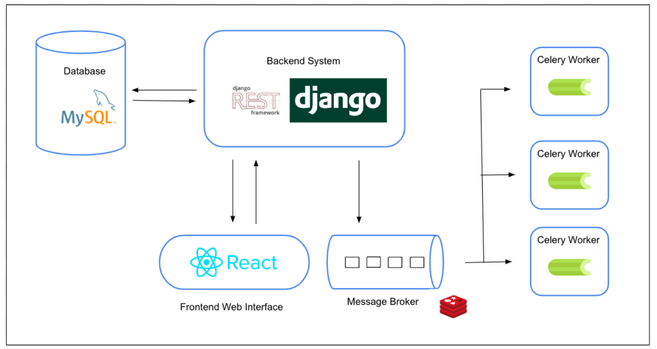
Digital Footprint Investigation is the process of identifying, processing, analysing, and reporting digital traces encompassing adversaries and targeted organizations to mitigate cyberattacks. However, the nature of manually searching for information from the Internet, the Dark Web, and Open-Source Intelligences has been time-consuming and inconsistent. The project aims to develop a Threat Intelligence platform that streamlines the Digital Footprint Investigation Processes.



Objectives

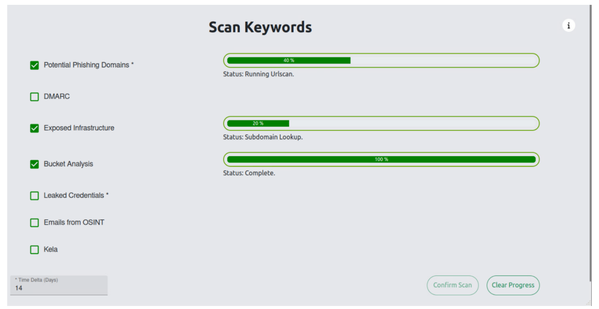
The primary objective of the Threat Intelligence Platform is to design and implement automation scripts for collecting, processing, and analyzing data within a centralized software. It aims to simplify data management, eliminate manual searches, and provide a centralized solution for analyzing cyber data from diverse sources, including the Dark Web, the Internet, and Open and Proprietary data sources, thus streamlining the whole Digital Footprint Investigation Process.

Methodology



The Threat Intelligence Platform implements a Three-Tier Architecture and an Asynchronous Distributed Task Queue Architecture. The backend server exposes API endpoints to handle database interactions, such as creating, reading, updating, and deleting terms from the MySQL Database, and delegates tasks to Celery workers via message brokers. These tasks come in the form of script functions that perform essential Digital Footprint Investigation processes. The workers asynchronously execute the tasks from the message broker and store the results in the MySQL Database to be retrieved by the backend server and shown in the user interface. The frontend interface also utilizes WebSockets to enable bidirectional communication with the backend server, facilitating real-time progress updates on script executions.

The Threat Intelligence Platform integrates seven Digital Footprint Investigation Scripts: Potential Phishing Domains that identify domain permutations mimicking legitimate organizations, Exposed Infrastructure that provides SSL certificates and external network footprint for vulnerability assessment, DMARC Policies for DNS record checking to enhance email security, Emails from OSINT that gathers relevant internal emails, Buckets Analysis that extracts misconfigured cloud asset management and buckets containing sensitive information, Leaked Credentials for email credentials, which can be exploited by attackers for unauthorized access, and the KELA Software Integration script collects compromised accounts and traces sources of data leaks from the dark web. Thus, these scripts facilitate digital footprint collection and risk and threat identification.



Conclusion

The Threat Intelligence Platform provides a centralized solution for managing data inputs, executing automation scripts, and viewing results, thus simplifying the Digital Footprint Investigation workflow.