Overview

Summary

- Cross references mentions of vendors, clients, and/or hardware (ex Microsoft) and keywords (ex. zero-day, hack, cyber attack) on individual sources (ex. news, message boards, etc) to monitor threats and breaches affecting a company.

Variables

- Sources
  - (ex. https://thehackernews.com/)
- Keywords
  - (ex. Malware, breach, 0-day, etc)
- Vendors
  - (ex. Microsoft, Cisco, Adobe)
- Client(s)
  - (ex. Core, BCBS, etc)
- Hardware/Software
  - (ex. Dell Latitude 1100, Zscaler, etc)

Connection to Other Apps

- Can send articles (URL) to News Capsule to be turned into a executive briefing report

Features

- Lists articles it has discovered
- Gives overview of emerging threats for user
- Notifies user of critical security threats
- Allows user to add/delete articles
- Allows user to filter articles
- Allows user to select and send articles to News Capsule app.

Pages

- Home/Article Dashboard Page
- Keywords Page
  - Includes 4 keyword lists:
    - Threat Keywords,
    - Vendors,
    - Clients,
    - Hardware/Software
- Sources Page

Workflow

1. User opens RisqAi and logs in (Container/Platform)
2. User navigates to Threat Tracker (Service/Application/App)
3. User (or background job) runs the application to find articles on Sources related to Keywords and cross-references them with the Hardware/Software, Clients and Vendors lists to see if their business is affected by threat.
    a. Application begins to process through list of Sources (URLs) -> follows the first URL for scraping
    b. Scraper opens Puppeteer
    c. Scraper scrapes raw HTML
    d. Scraper sends raw HTML to OpenAI to detect the HTML element that the body copy is stored in
    e. Scraper scrapes remaining articles based on structure detected in 1st scrape
    f. Scraper sends article content to OpenAI to find relative cross-referenced keywords
    g. Open AI reads article and finds keywords
    h. Open AI sends back structured JSON of results Title, Author, Summary, Detected keywords and article
    i. Scraper stores results in database (URL, Title, Author, Summary, Detected keywords, Scrape Date)
4. User is presented with a list of found articles (URL, Title, Author, Summary, Detected keywords, Scrape Date)

Tech Stack

- React
- React Router
- Tailwind
- PostgressDB
- Puppeteer
- Vite
- ShadeCN
- Tanstack
- NodeJS
- Drizzle
- Socket.io