PWC

Система предоставления информации по IT безопасности

Контекст / описание проблемы:

Киберсообщество растет все быстрее, но сегодня для принятия решений в случае киберугрозы недостаточно знания основных тенденций. Например, первые сообщения, касающиеся вымогателя WannaCry, были опубликованы в социальных сетях за 6 часов до официального объявления о нём в средствах массовой информации. Если бы эта информация была широко распространена вовремя, многие компании успели бы принять соответствующие меры или просто отключить сервисы.

Компаниям необходим быстрый способ получения информации о текущих тенденциях, новостях и проблемах в области информационной безопасности. Информация нужна им сейчас. Поэтому мы предлагаем вам создать программное обеспечение, которое будет собирать статьи, блогпосты, сообщения в чатах в Твиттере, Facebook, Telegram, из Даркнета и средств массовой информации и анализировать их.

Задача:

Проведение исследований в области анализа данных, полученных из социальных медиа, и разработка программного обеспечения, способного в онлайн-режиме собирать в социальных сетях темы, касающиеся информационной безопасности, и анализировать их.

Основная цель этого приложения - создать простой, интуитивно понятный и постоянно обновляющийся источник информации о текущем состоянии информационной безопасности.

Эта задача также может включать в себя исследования характеристик информационных потоков, таких как скорость/длина/количество постов и др. Например, это может быть исследование корреляции количества постов на специализированных форумах в Даркнете в дни с крупными инцидентами безопасности.

Требования к решению:

Проанализировать возможные методы решения задачи и разработать программное обеспечение (веб-приложение), удовлетворяющее техническим требованиям, указанным ниже.

Подготовить презентацию разработанного решения. (ppt)

Технические требования к решению:

Программное обеспечение (веб-интерфейс), должно быть способно:

а) Собирать данные об информационной безопасности из различных источников, включая, но не ограничиваясь:
- блоги по информационной безопасности
- facebook;
- twitter;
- telegram;
- специализированные форумы в Даркнете (Darknet)
- источники в средствах массовой информации

Мы предлагаем вам начать с 50 лучших авторов из этого списка.

б) Оценивать текущие тенденции в области информационной безопасности посредством анализа собранных данных.

в) Представлять результаты через графический пользовательский интерфейс (через веб-браузер) в формате, прозрачном для бизнеса.

Критерии оценки:

- Критерий: Понятность для бизнес-пользователей
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Критерий: Масштабируемость приложения
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Критерий: Производительность - менее 15 минут на анализ новой статьи
  Шкала оценки: максимальный балл - 5, минимальный балл - 1
- Критерий: Дальнейшие пути развития системы
  Шкала оценки: максимальный балл - 5, минимальный балл - 1