

MICHIGAN STATE

UNIVERSITY

Beta Presentation Open Source Intel

The Capstone Experience

Team GM

Ben Buscarino

Will Crecelius

Igli Ndoj

Qiming Ren

Taylor Zachar



*From Students...
...to Professionals*

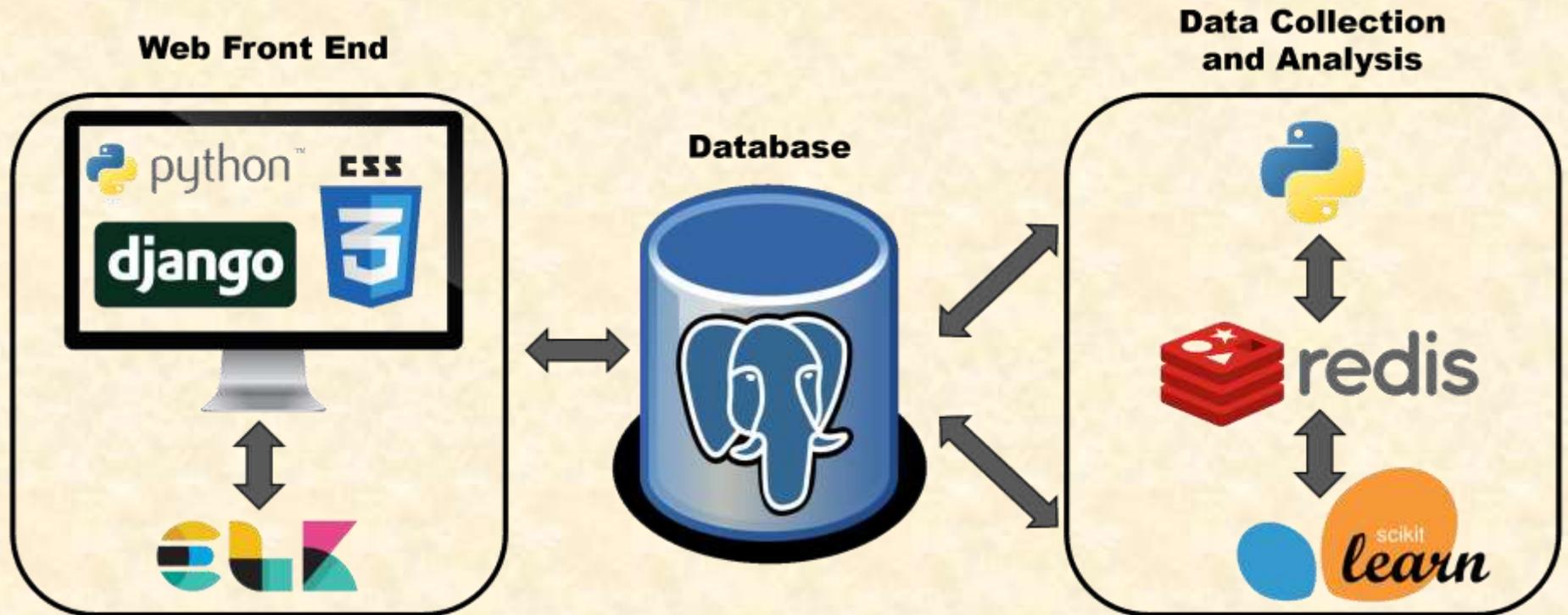
Department of Computer Science and Engineering
Michigan State University
Spring 2019

Project Overview

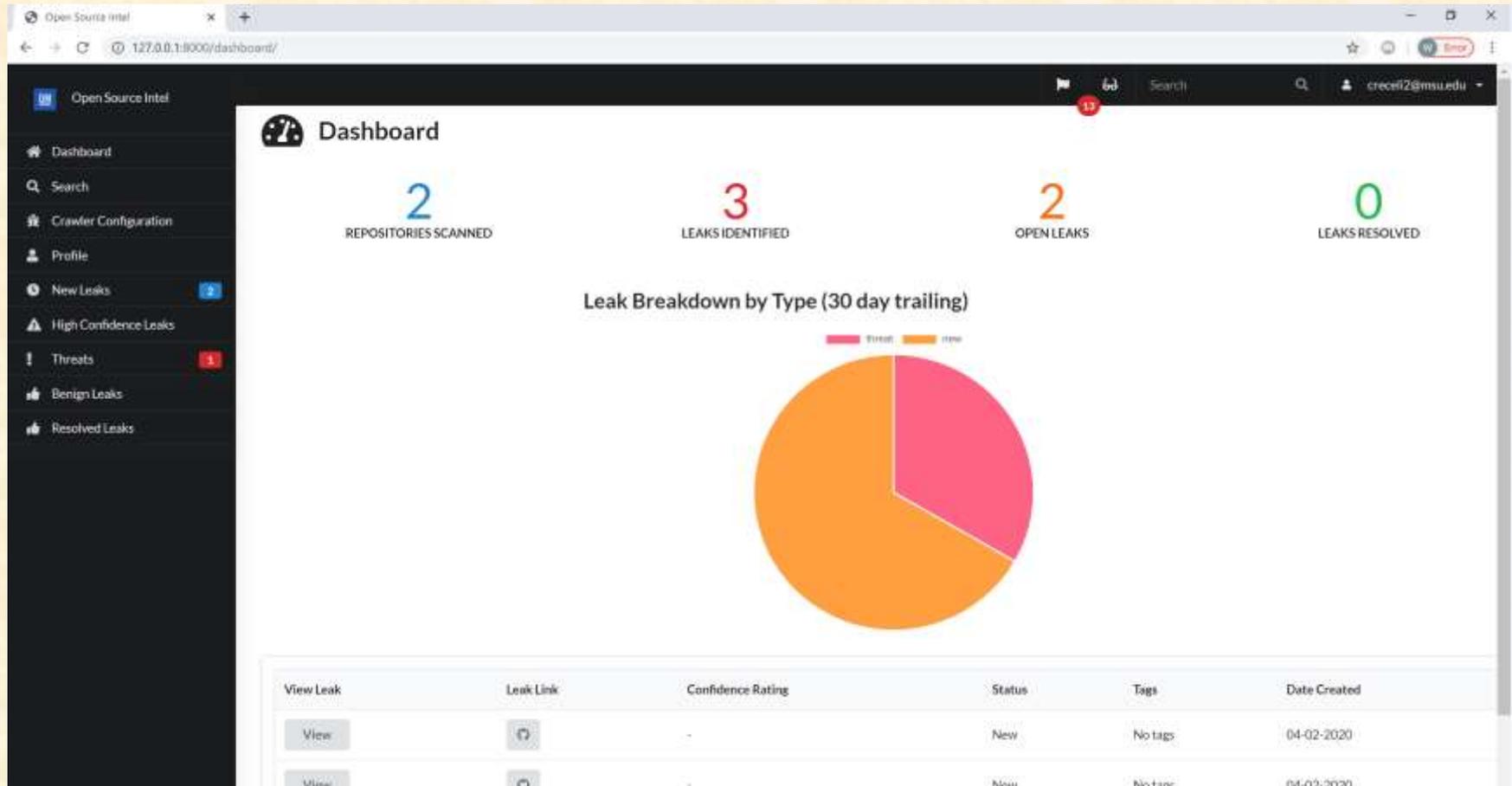
- Scan public repositories such as GitHub, PasteBin, and Bitbucket for leaked GM intellectual property.
- Assign a confidence rating to a leak using machine learning.
- Display the leaks and provide URL to the leaks in a frontend web application.



System Architecture



Dashboard



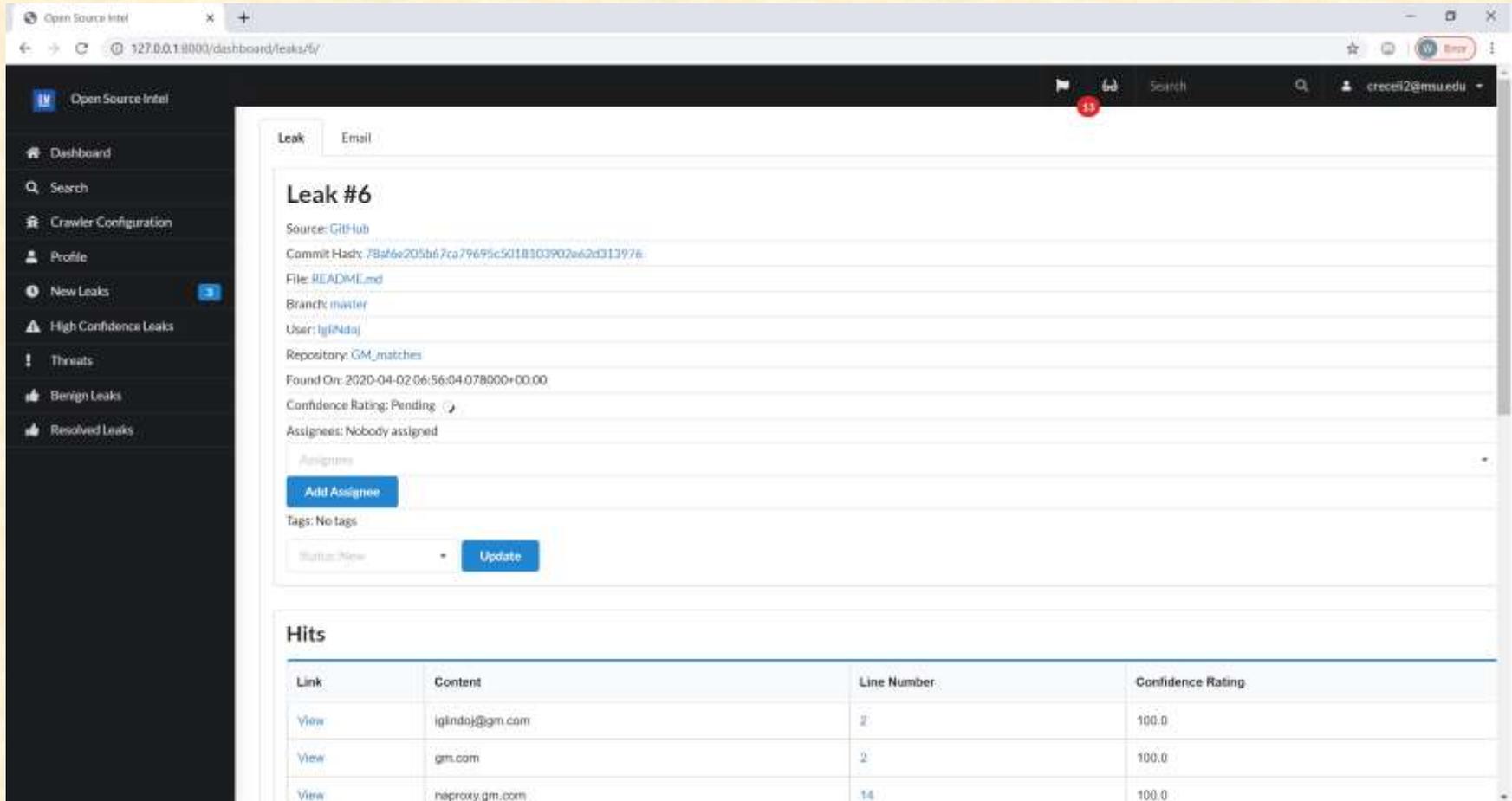
Leaks Page

The screenshot shows a web browser window with the URL `127.0.0.1:8000/dashboard/leaks/?status=new`. The page title is "New Leaks". At the top, there are four summary cards: "LEAKS DETECTED" with a value of 3, "NEW LEAKS" with a value of 3, "HIGH CONFIDENCE LEAKS" with a value of 0, and "RESOLVED LEAKS" with a value of 0. Below these cards is a table with the following columns: "Leak ID", "Leak Link", "Status", "Date Created", and "Date Discovered". The table contains three rows of data, each with a leak ID (1, 5, and 6), a link icon, and the status "No Tags". The "Date Created" for all three is "04-02-2020", and the "Date Discovered" is "04-05-2020" for ID 1 and "04-02-2020" for IDs 5 and 6. At the bottom of the table, it says "Page 1 of 1".

Leak ID	Leak Link	Status	Date Created	Date Discovered
1		No Tags	04-02-2020	04-05-2020
5		No Tags	04-02-2020	04-02-2020
6		No Tags	04-02-2020	04-02-2020



Single Leak Page



The screenshot shows a web browser window displaying the 'Single Leak Page' in the Open Source Intel application. The browser's address bar shows the URL `127.0.0.1:8000/dashboard/leaks/6/`. The application's navigation sidebar on the left includes links for Dashboard, Search, Crawler Configuration, Profile, New Leaks (with a notification badge), High Confidence Leaks, Threats, Benign Leaks, and Resolved Leaks. The main content area features a 'Leak #6' header and a 'Leak' tab. The leak details are as follows:

- Source: GitHub
- Commit Hash: `78af6e205b67ca79695c50118103902e62d313976`
- File: `README.md`
- Branch: `master`
- User: `iglindoj`
- Repository: `GM_matches`
- Found On: `2020-04-02 06:56:04.078000+00:00`
- Confidence Rating: Pending
- Assignees: Nobody assigned

Below the details, there is an 'Assignees' section with an 'Add Assignee' button, and a 'Tags' section with 'No tags'. At the bottom of the details, there is a 'Status: New' dropdown and an 'Update' button. The 'Hits' section contains a table with the following data:

Link	Content	Line Number	Confidence Rating
View	<code>iglindoj@gm.com</code>	2	100.0
View	<code>gm.com</code>	2	100.0
View	<code>reproxy.gm.com</code>	14	100.0



Crawler Configuration Page

The screenshot displays the 'Regex Configuration' page in the Open Source Intel application. The page features a sidebar with navigation options and a main content area with a table of configurations. The table includes columns for the regex pattern, title, active status, and various options like 'ascii', 'multi line', and 'dot all'. Each row also has 'Update' and 'Drop' buttons.

Pattern	Title	Active	ASCII	Multi Line	Dot All	Update	Drop
		<input type="checkbox"/>				Insert	
192.208\.(?25 0-6)?20-	GM IP Address	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Update	Drop
[?wv-]+@[?!(?wv- +\\ !)?p	GM Email Address	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Update	Drop
[?@IP(?wv- +\\ !)?gm]gr	GM Domain	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Update	Drop
\\b(?nam\\)?A-z]?zZ[A-z]	GM Z-ID	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Update	Drop
{7.onstar cadillac chevro	Password	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Update	Drop
shop{1,2}click{1,2}driv	shop_click_drive	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Update	Drop
7458bc2ad18e6417f0e	Hex	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Update	Drop
import.com,onstar,	DrStar Java Import	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Update	Drop



What's left to do?

- Test software with our client
- U.I. debugging
- Improving U.I. flow
- Train ML, as we confirm more leaks



Questions?

?

?

?

?

?

?

?

?

?

