

MICHIGAN STATE

UNIVERSITY

Beta Presentation

AI Cyberattack Early Warning System

The Capstone Experience

Team Vectra AI

Alex Fortsch
Graham Holley
Ajay Kumar
Morphane McAnelly
Aleksa Popovic
Jacob Sock

Department of Computer Science and Engineering
Michigan State University

Fall 2024



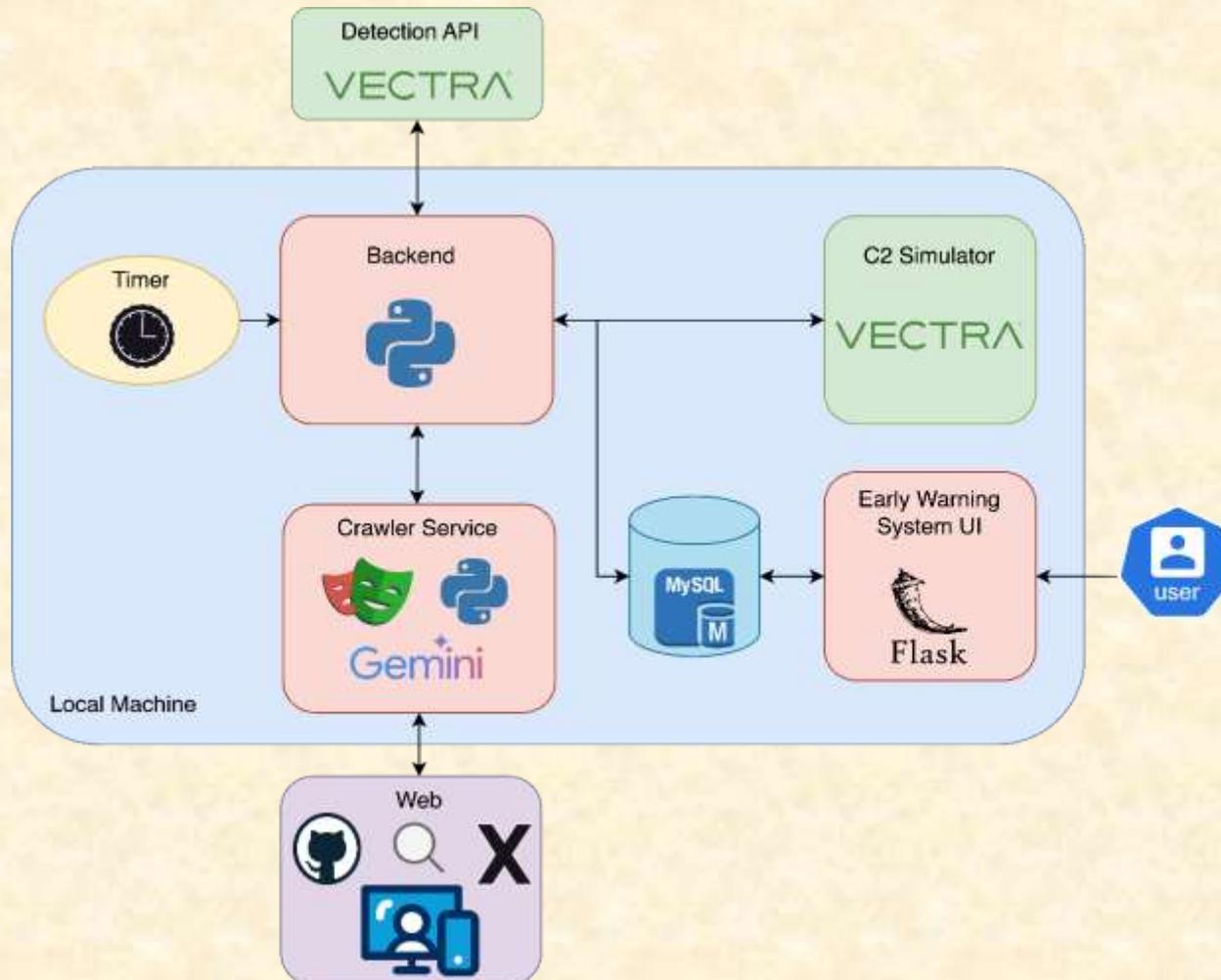
*From Students...
...to Professionals*

Project Overview

- Problem
 - Data scientists have to manually read reports and configure the C2 simulator
- Solution
 - Automate the process by web scraping threat intel resources, extrapolating C2 configs, and generate PCAP samples
- Result
 - Human intervention in the process is eliminated



System Architecture



User Interface

The screenshot shows a web browser window with the URL <https://www.vectra.ai/AutomatedSimulations>. The page title is "AI CYBERATTACK EARLY WARNING SYSTEM".

Simulation Timer
00:00:01

Start **Scrape all of DFR** **Scrape Twitter**

Enter a URL to scrape

Enter URL here

Add to URL Scraping Queue

Select a Category

- Website
- Google

Jobs in Backend
Number of Jobs: 0

Relevancy

Positive	Negative	Total	Positive %
50	10	60	83%

Gemini Generation

Positive	Negative	Total	Success %
40	20	60	67%

C2 Results

Positive	Negative	Total	Success %
44	16	60	73%

Monitored URLs | Processed Jobs | Monitored Tools

Monitored URLs

URL	Category	Status
https://thedfirreport.com/2023/06/12/a-truly-graceful-wipe-out/	Website	Waiting



User Interface

Monitored URLs	Processed Jobs	Monitored Tools
Monitored URLs		
URL	Category	Status
https://thefirreport.com/2023/06/12/a-truly-graceful-wipe-out/	Website	Waiting

Simulation Timer

00:00:01

Enter a URL to scrape

Select a Category

- Website
- Google

Jobs in Backend
Number of Jobs: 0



User Interface

The screenshot shows a web browser window with the URL <https://www.vectra.ai/AutomatedSimulations>. The page title is "AI CYBERATTACK EARLY WARNING SYSTEM".

Simulation Timer
00:00:00

Buttons: Stop, Scrape all of DFIR, Scrape Twitter

Enter a URL to scrape:
Add to URL Scraping Queue

Select a Category:
• Website
• Google

Jobs in Backend
Number of Jobs: 0

Relevancy				Gemini Generation				C2 Results			
Positive	Negative	Total	Positive %	Positive	Negative	Total	Success %	Positive	Negative	Total	Success %
50	10	60	83%	40	20	60	67%	44	16	60	73%

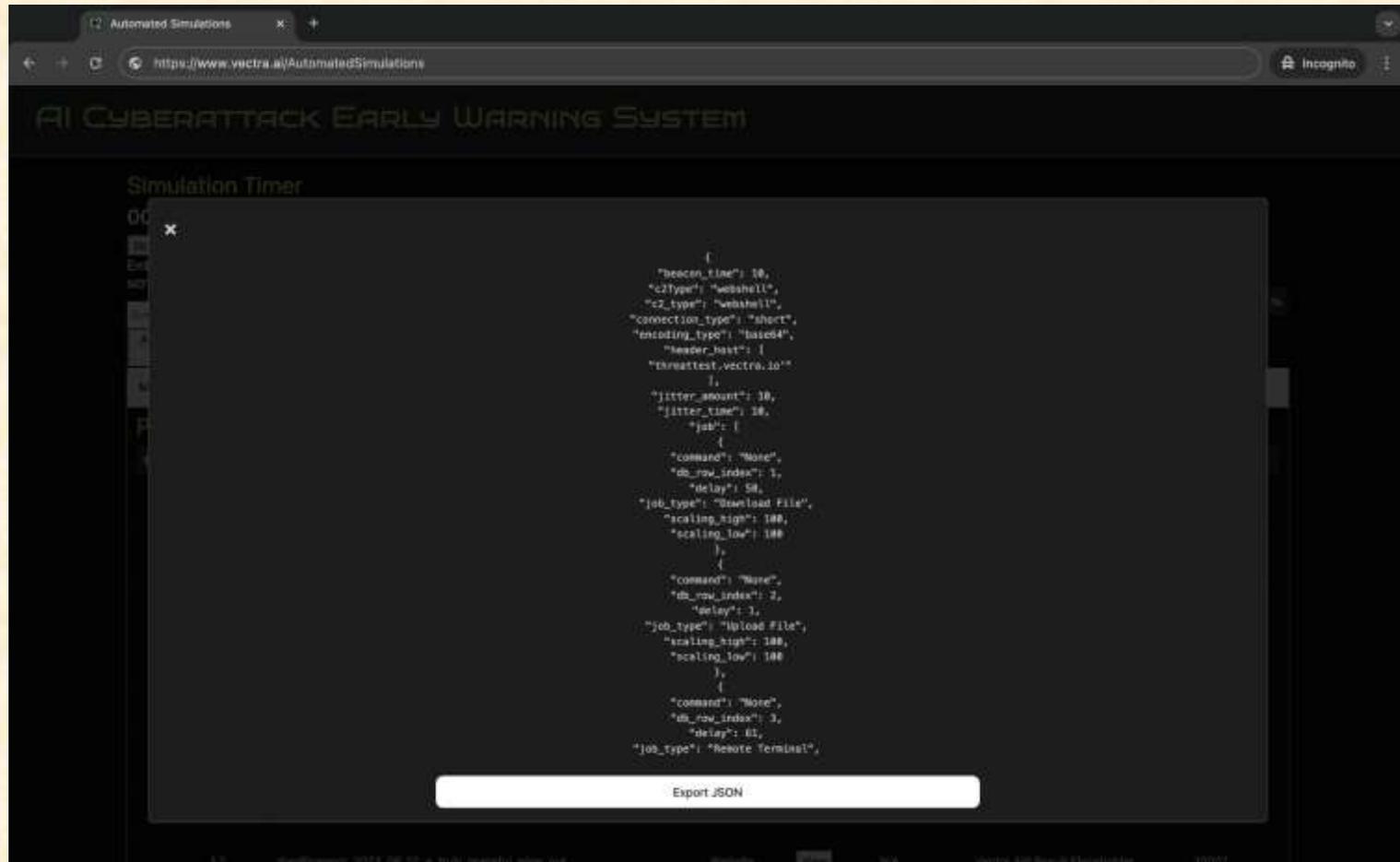
Monitored URLs | Processed Jobs | Monitored Tools

Processed Jobs

Toggle	Job #	URL	Category	Properties	C2 Result	Vectra API Result	Port Number
<input type="checkbox"/>	1	https://thefirreport.com/2023/06/12/a-truly-graceful-wipe-out/	Website	View	Complete	Success	10000



User Interface



User Interface

The screenshot displays the user interface for the AI Cyberattack Early Warning System. The page title is "AI CYBERATTACK EARLY WARNING SYSTEM".

Simulation Timer: 00:00:04

Controls: Stop, Scrape all of DFIR, Scrape Twitter, Enter a URL to scrape, Select a Category (Website, Google), Jobs in Backend (Number of Jobs: 0), Add to URL Scraping Queue.

Relevancy and Gemini Generation Results:

Relevancy			Gemini Generation				C2 Results				
Positive	Negative	Total	Positive %	Positive	Negative	Total	Success %	Positive	Negative	Total	Success %
60	10	60	83%	40	20	60	67%	44	16	60	73%

Monitored Tools:

Tool Name	Url	Version	Last Ran	Run Tool
Rubeus	https://github.com/SecWiki/rubeus	1.0	2024-09-20 12:00	[Run]
LDAP Domain Dump	https://github.com/SecWiki/randomdump	2.0	2024-09-18 07:30	[Run]
Certify	https://github.com/SecWiki/certify	2.1	2024-09-16 09:00	[Run]
ADFind	https://www.sagemat.net/foretools/foosad/foad/	2.05	2024-09-13 10:30	[Run]



What's left to do?

- Stretch Goals
 - Visualize PCAP data
 - Gemini default usage percentage
 - Add additional known tools
- Other Tasks
 - Integrate with Vectra AI's VM
 - Refactor code



Questions?

?

?

?

?

?

?

?

?

?

