MICHIGAN STATE UNIVERSITY Project Plan Presentation AI Cyberattack Early Warning System The Capstone Experience

Team Vectra Al

Alex Fortsch Graham Holley Ajay Kumar Morghane McAnelly Alex Popovic Jacob Sock

Department of Computer Science and Engineering Michigan State University

Fall 2024



From Students... ...to Professionals

Project Sponsor Overview

- Cybersecurity Monitoring Company
 - Founded in 2011
- Pioneers of Generative Al
- Attack Signal Intelligence
 - Monitor attacks WITHOUT decryption
 - Machine learning to detect attacks and offer solutions
- Past Michigan State Capstone Sponsors
 C2 simulator

The Capstone Experience

VECTRA

Project Functional Specifications

- 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

Project Design Specifications

- Users should be able to pass in a URL in through a user interface
- Users should know the current URLs in the queue and ones already being monitored
- Users should be able to see the results of run C2 Simulator
- Users should be able to run other detection tools with valid configurations
- Users should be able to see the statistics of how the application is working as well as success rates

Screen Mockup: Opening Screen

SZ. Anto	imated Structures X: +					
	C 0 127.0.0.1.5000/AutomatedSime	ulations			ए. 🕁 🔒 Incogni	to New Chrome evaluable
Co Mau						C3 All Bookmu
Co	MMAND AND CON	TROL SIMULA	ITOR			
	Simulation Timer					
	00:00:03 Enter a URL to scrape	Select a Category	Scraper/LLM	C2 Simulator	Monitored Tools	
	Enter URL here	Website Google Alert			Success % Successes Failures Tota	al Success %
	Add to URL Scraping Queue	• Twitter	50 10 60	25 5 30	10 2 12	
	Monitored URLs Processed Jobs	Monitored Tools				
	Monitored URLs					
	Lat.		Category		Status	
	https://example.com/		Automatic Website		Scraping	
	https://example2.com/		Automatic Google Alert		Wetting	
	https://esample3.com/		Automatic Twitter Alert		Walling	
			User inputied Website URL		Walling	



Screen Mockup: Processed Jobs

wated fi	imulations × +											
σ	@ 127.0.0.1.5000/Automated5	Imulations							٩	* #	Incognito New Chron	me avi
											14	
mm	IAND AND CO	NTROL SIMULATO	DR									
ç	Simulation Timer 00:00:07 Enter a URL to scrape	Select a Category	Scrap	er/LLM		C2 Simu	alator		Мо	nitored Te	ools	
	Enter 1341, here	Website Google Nert		Negative		e 14 Successes	Failures	Total Su			es Total Success %	
	Add to URL Scraping Queue	Twitter	50	10		1923	12	: ::::::	10	2	12	
	Monitored URLs Processed Jobs	Monitored Tools		12	60	25	6	30		-	1	1
	Monitored URLs Processed Jobs Processed Jobs URL	Monitored Tools	11	Article Name		Category		Properties	C2 Job Status	Vectra	Last Reft	
	Processed Jobs	Monitored Tools	11						C2 Job	Vectra		
	Processed Jobs un: https://www.com/	Monifored Tools		Article Name		Category		Properties	C2 Job Status	Vectra Detected	Last Ran 2024-08-14	
	Processed Jobs URL https://www.com/ https://www.com/ https://www.com/2024/00/1 ecretal		-batch-	Article Name Example Art Threat Actor		Category Automatic We User inputted		Properties	C2 Job Status Consided	Vectre Detected	Last Ren 2024-09-14 11:00 2024-09-13	

Screen Mockup: Simulation Config

IMAND AND CONTROL SIMULATOR				
Simulation Properties	Playbook			
Simulation Name	Job Type	Content	Delay	Scaling
Log job subject to the	Liptost File		(15)	10%-20%
■ Webshall Protectel ● TCP ● HTTP ● HTTPS ● LIDP ● WebSackel ● HTTP/2 ● HTTP/3 ● REST	Portiscen			80%-100%
View Matheotice Profile	Download File			70%-100%
Server Underling Port:	Arbitrary Command	pwd	ta	60%-100%
Beacon time: seconds	Artenary Communa	tiwa		60%-300%
Jittier: seconds				
Beacco Type: Dynamic Beaccoing				
- Padding Type: ● Flat ● Random Connection Profile: ● Long ● Short				
Encoding Type • Traditional • Base64				
Number of Turinela:				

Screen Mockup: Monitored Tools

67 Automa	ited Simulations X														
€ 9 9	3 @ 127.0.0.1:5000/	AutomatedSimulations									Q, 🖈	t∰ in	cognito	New Chrome av	silable
C3 MSU															lookitist
Con	IMAND AN	CONTROL SIM	ULATOR	5											
	Simulation Til 00:00:05 Enter a URL to scrape Enter GRL twee				er/LLM	Total Postive 9	C2 Sim		Total		Monitor			ineens %	
	Add to URL Scraping Que			50	10	60	25	5	30.		10	2	12		
	and the second second second			**		00		1	240		18	÷	15		
		ocessed Jobs Monitored Tools													
	Monitored To														
	Tool Name	URL	Version		iel Ansult		Vectra Dete	ted		Last R					
	Tool A		1.0	3	Completed		Success			2024	-09-14 16-3	0)			
	Tool B		25	ŝ	failed.		NA			2024	-09-14 15:0	0			
	Tool C		1.5		Completed		Failed			2024	-09-14 13:4	5			
	Tool D		2.0		Falled		NK			2024	-09-14 12:0	0:			
	Tack II		**		Completed		Success			2024	-09-13 15:0	0,.			
	Tool F		19	ä	Failed		NPA			2024	-09-13 14:3	0			
	Tool G		2.5	3	Completed		Success			2024	-09-13 13:0	o i			
	Tool H		2.7	į	Failed		NØA			2024	-09-13 1142	6			

Screen Mockup: Statistics

	Automated Simulations N										
Command and Control Simulator Simulation Timer 00:00:02 Enter a URL to scrape • Website • Coccels Allert • Occels Allert • Website • Coccels Allert • Website • Occels Allert • Occels Allert <th>- C @ 127.0.0.1-5000</th> <th>AutomatedSimulations</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>a, 🕁</th> <th>A Inco</th> <th>sgnite New Chr</th> <th>ome availabl</th>	- C @ 127.0.0.1-5000	AutomatedSimulations						a, 🕁	A Inco	sgnite New Chr	ome availabl
Simulation Timer 00:00:02 Enter a URL to scrape Select a Category Wokale Enter AURL to scrape Occup Alert Add to URL Scraping Quoue Tritter URL Scraping Quoue Tritter Total Success 14 Buccesses Failures Total Success 14 Buccesses 1	MSU										🗁 All Beicke
Scraper/LLM C2 Simulator Monitored Tools Enter a URL to scrape • Webnite • Google Alert • Google Alert • Trate URL to scraped Queen • Webnite • Google Alert • Total • Total to URL Scrapeling Queen • Webnite • Google Alert • Total • Total to URL Scrapeling Queen • Total total • Google Alert • Total	Command an	CONTROL SIMUL	ATOR								
Enter a URL to scrape Select a Category Website Cocgle Alert Website Cocgle Alert Total Positive Negative Total Positive Negative Total Positive Negative Total Success 1 Buccess 1 Bucces 1 Buccess 1 Bucces 1 Buccess 1 Buccess		mer									
Enter Life. here Coccele Alert Positive Negative Total Successes Failures Total Successes			Scrape	er/LLM	C2 Sim	ulator		Monitor	ed Tool	s	1
20 10 80 25 8 30 10 2 12		Google Alert	Positive	Negative Total	Postive % Successes	Failuren Tot	d Success %	Guccesses	Failures	Total Success %	
Monitored URE & Processed Jobs Monitored Tools	Add to OKL Scripping Qu		10	10 60	25	5 3	ii.	10	<u>36</u>	Seale -	
	Monitored URLs P	rocessed Jobs Manitared Tools									-
	Monitored LPELs P	rocessed Jobs Manitaned Taals					-				
	Monitored LPELs P	rocessed Jobs Manitared Tools					-				J
	Monitored LPELs P	rocessed Jobs Monitored Tools									
	Monitored UPLs P	rocessed Jobs Monitored Tools									

Project Technical Specifications

- Playwright and Python to scrape HTML content
- Gemini LLM to extract C2 configuration parameters
- Frontend built using Flask, HTML, CSS, and Jinja
- Backend and connector code written in Python
- MySQL for data storage

Project System Architecture



Project System Components

- Hardware Platforms
 - Computers
- Software Platforms / Technologies
 - Playwright
 - Gemini
 - Flask
 - VSCode
 - Pyshark
 - MySQL
 - Python

Project Risks

- Website Accessibility
 - Some URLs require authorization we don't have
 - Human manned accounts as well as utilizing alternative data sending from sources that have it
- Website Content Filtration
 - Certain websites contain tags that will not be standardized
 - We can utilize our LLM to ignore the tags in the summary
 - We can develop a filtration system within our webscraper
- Automation of Cyberattack Tools
 - Cyberattack tools that are parsed in by the user need to be ran without being known
 - We can make use our LLM to find out how to run any given tool and then use Argparse to run the commands that the LLM returns
- High Cost of LLM Model Tiers
 - Calling the API for LLMs can be very pricey and our project triggers the "high risk" filters
 - We need to prompt engineer and change data so that our prompts won't get an invalid call

Questions?

