### MICHIGAN STATE UNIVERSITY Project Plan Presentation Hybrid Cyberattack Simulator

#### The Capstone Experience

#### Team Vectra Al

Henry Barton Alisha Brenholt Nathan Motzny Campbell Robertson Andrew Talbott

Department of Computer Science and Engineering Michigan State University

Spring 2024



From Students... ...to Professionals

#### **Project Sponsor Overview**

# VECTR۸

- Leader in Cybersecurity
- Focus on network security
- Utilizes AI to detect, investigate, and report attacks
- Modular security to provide customized coverage

### **Project Functional Specifications**

- Vectra's AI models need relevant training data to maintain accuracy
- Several more network protocols and hybrid attack capabilities are being added to the Command & Control (C2) Simulator
- Vectra will be able to prepare for diversified attacks using many different protocols and attack vectors

### **Project Design Specifications**

- Hybrid Attack Simulation
  - MAAD-AF
  - DeRF
- Advanced C2
  - Webshells
  - Beaconless servers
- UI Enhancements

### Screen Mockup: Simulation Overview with Playbook Display

Simulation	Test Sim									
Start Tin 2024-01-29 11		Protocol N http	lumber of Tunnels 1	Connect	<b>ion Type Bea</b> ng	con Time	Jitter Amount	Pedding Type Random		Amount 0
Logarithmic Scal		Pc	ap Dr	та			Playboo	ok Traffic Br	owser	
70,000							Job Typ	e Delay	Status	Display
60,000			Packet	D 51			- Upload F	ile 3	complete	
50,000	12		Data Siz	• 65539						
v 40.000	Јов Тур	e Upload File	Capture	11:35:47	Beacon Number	4	Portsca	n 3	complete	18
— 000,00 B	Start Ti	me 11:35:42	a server	J	Beacon Time	11:35:52.127				
	Delay	5			Interval Amount	2.176				
20,000	Status	Complete			Interval Change	-0.33s				
10,000					1					
18:43:05.000	18:43:07.000	6:43:09.000 18:	.43:11.000 18		18:4 <sup>3</sup> :15.000 18:4 <sup>4</sup>	3:17.000				

### Screen Mockup: Simulation Overview with Browser Display

Start Time     Port     Protocol     Number of Tunnels     Connection Type     Beacon Time     Jitter Amount     Padding Type     Padding Amount       2024-01-29 18-8129     9000     http:     1     long     3     1     Rendom     0       Legarithmic Scale     PCAP DATA     Playbook     Traffic Browser     Filters       70,000     0     0     0     0     0     0       60,000     Data Size     65399     Cepture     113547     Size     Time     Sender       30,000     20,000     0 <th>2024-01-29 18:41:29     9000     http     1     long     3     1       Cogarithmic Scale     PCAP DATA     Playbool     Packet ID     50     50     50     50     51     50     51     50     51     50     51     50     51     50     50     51     50     51     50     50     51     50     51     50     51     50     51     50     50     51     50     51     50     50     51     50     50     51     50     50     51     50     50     51     50     50     51     50     51     50     51     50     51     50     51     50     51     50     51     50     51     51     51     51     51     50     51</th> <th>Random k Traffic I Size 44</th> <th>Browser Time 1843:10.317</th> <th>0 Filters Sender server</th>	2024-01-29 18:41:29     9000     http     1     long     3     1       Cogarithmic Scale     PCAP DATA     Playbool     Packet ID     50     50     50     50     51     50     51     50     51     50     51     50     51     50     50     51     50     51     50     50     51     50     51     50     51     50     51     50     50     51     50     51     50     50     51     50     50     51     50     50     51     50     50     51     50     50     51     50     51     50     51     50     51     50     51     50     51     50     51     50     51     51     51     51     51     50     51	Random k Traffic I Size 44	Browser Time 1843:10.317	0 Filters Sender server
Picap Data     Playbook     Ifattic Browser     Filters       70,000     0     51     50     51     50     44     1843:10.317     sender       50,000     0     0     53     40,000     11.35:47     50     44     1843:10.317     senver       50,000     0     0     0     11.35:47     51     605399     18:42:10.338     client       50,000     10,000     0     11.35:47     52     3162     18:42:11.386     client       10,000     1	PCAP DATA     Playbool       70,000     Packet ID     51       60,000     Data Size     65539       50,000     Capture     10 to 10 to 10	44	Time 18:43:10.317	Sender
70,000   Packet ID   51     60,000   Data Size   65539     50,000   Capture   11:35:47     50,000   Capture   11:35:47     50,000   Size   Size     50,000   Capture   11:35:47     50,000   Capture   11:35:47     50,000   Size   Size     50,000   Size   Size     50,000   Capture   11:35:47     50   14   18:43:10.317     52   3162   18:43:11.186     60,000   Size   Size     52   3162   18:43:11.186     60   B:43:01.000   B:43:15.000     18:43:01.000   B:43:15.000   B:43:17.000     18:43:01.000   B:43:13.000   B:43:15.000     18:43:01.000   B:43:15.000   B:43:17.000	70,000     Packet ID     51     50       50,000     Capture     Capture     51     50	44	Time 18:43:10.317	Sender
50,000   Deta Size   65539     50,000   Capture   11:35:47     50,000   S2   3162     50,000   18:43:10.100     10,000   18:43:10     10	50,000 Data Size 65539 50,000 51			
50,000 20,000 20,000 10,000	50,000 Capture	00539	18:43:10.538	
10,000 10,00		1994555		
20,000 10,000 10,000 10,000 10,000 10,000 18:43:0 <sup>1</sup> ,000 18:43:1 <sup>1</sup> ,000	奋 30,000	3162	18:43:11.186	1.000
10,000 10,000			New Street	
18:43:05.000 18:43:01.000 18:43:11.000 18:43:13.000 18:43:17.000 18:43:17.000 18:43:17.000 18:43:17.000 18:43:100 18:43:100 18:4001 18:400000000000000000000000			Edit	t Filters
18:43:05.000 18:43:01.000 18:43:11.000 18:43:13.000 18:43:15.000 18:43:17.000 Size 18:43:15.000 18:43:10 18:43:10 18:43:15.000 18:43:15.000				
18 <sup>:A,r</sup>	305,000 3.01,000 3.01,000 3.13,000 3.15,000 3.11,000			ize
	18: <sup>A3*</sup>		- Je	əb



### Screen Mockup: Create Simulation Page

C Coste Sinulation	• + D • 1270814-000 Noveline comm		e 19 A	× × = **** <b>5</b> 0 0
Comman	ID AND CONTROL SIMULA	TOR		
Simu	ulation Properties	Playbook		
Simula	ation Name:	Add Camonand		
	ot • TCP • HTTP • HTTPS • UDP • WebSacket • HTTP/2 • HTTP/3	Job Type	Delay A	Actions
Advan	cod C2; = Beaconless = Webshall n time:seconds	+ New Command Command Type:		
Jitter:	seconds Ig Type: ● Flat ● Random	Portscan Opwnload File		
	ction Profile: • Long • Short	Upload File Dump Configuration Remote Task		
Numb	er of Tunnels:	Active Directory Scanning Eclificate Data		
		Encrypt File System InterCommund Delay		
		Remote Terminal Kity Logger		
		Arbitrary Command OreRF Job MAAD-AF Job		
		EXECUTE RECON		
		Olelay: 0 seconds		
				Cercel



# Screen Mockup: Simulation Overview Page

Simulation C	verview			
Simulation Name	Port	Status	Start Date	Actions
Test Sim	9000	ended	2024-01-29 18:41:29	( Manuel Little   Channel   Colorent Log
idsa	8009	ended	2024-01-29 18:50:32	Weer / Latz Dans Delete OpenLog
				Here Dans Here
				Improve parts     Microsoft Statement     Expression     Improve parts     Impro
			-	ې چې د معموم د اول مېلو کې د د د د د د د د د د د د د د د د د د
				Time PC     Name     Determative     Type     Soc       2 80 Objects     Ω Nospien     V2V2004 Indi Finit     XOIn Finit     0.00       Beckhop     Ω Taxt Simpon     V2V2004 Indi Finit     XOIn Finit     0.00       Decements     Decements     0     0.00     0.00       Maric       0     0.00     0.00       Maric        0     0.00     0.00     0.00

### **Project Technical Specifications**

- Implementing WebSocket, HTTP/2 and HTTP/3
- Also adding MAAD-AF and DeRF frameworks for Hybrid Attacks
- PyShark library to capture network packets, and MySQL to store them
- All of this is built on Python3

### **Project System Architecture**



### **Project System Components**

- Hardware Platforms
  - AWS Server
  - Google Cloud Server
  - Two Lab PCs
- Software Platforms / Technologies
  - Python
  - MySQL
  - Flask
  - VSCode

### **Project Risks**

- Compatibility
  - Make sure all third-party apps work together
  - Using active libraries and using version control
- Generating realistic data
  - Generate realistic enough data for AI models to train on
  - Analyzing real world attacks and mimicking their outputs
- Performance Issues
  - Make large amounts of data in reasonable amounts of time
  - Spending time optimizing code; looking at distributed computing
- Portability
  - The program needs to be able to run on multiple OS without issue
  - Using cross-platform libraries and allowing API calls to server to abstract user operating system

### **Questions?**

