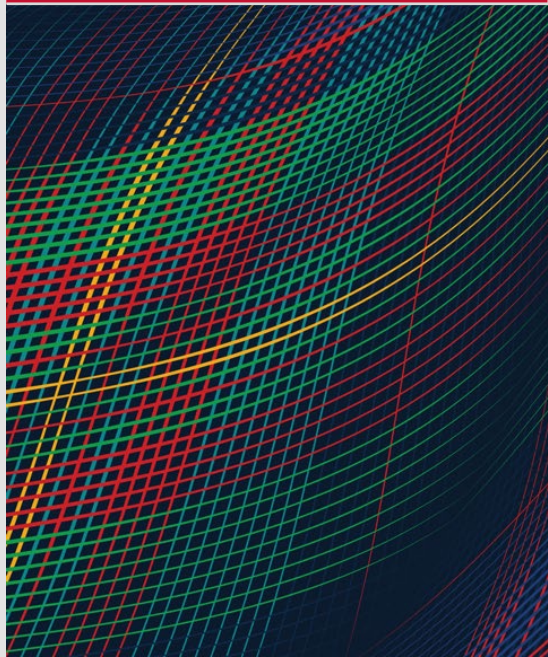
Carnegie Mellon University
Software Engineering Institute



Improving Cyber Mission Readiness: The Power of Team Exercises with Emerging Technologies

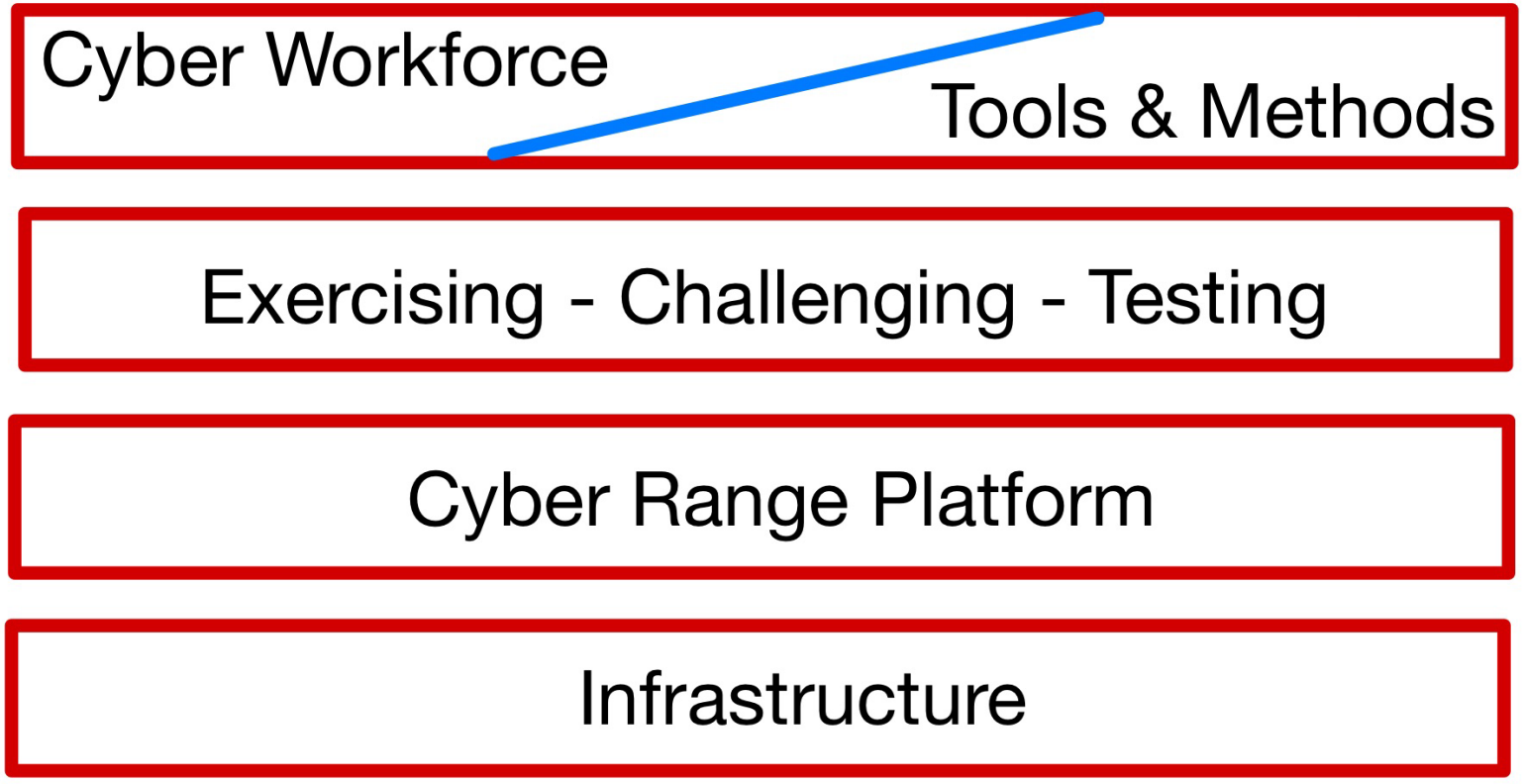
AUGUST 24, 2023

John Yarger, Tom Podnar, Dustin Updyke

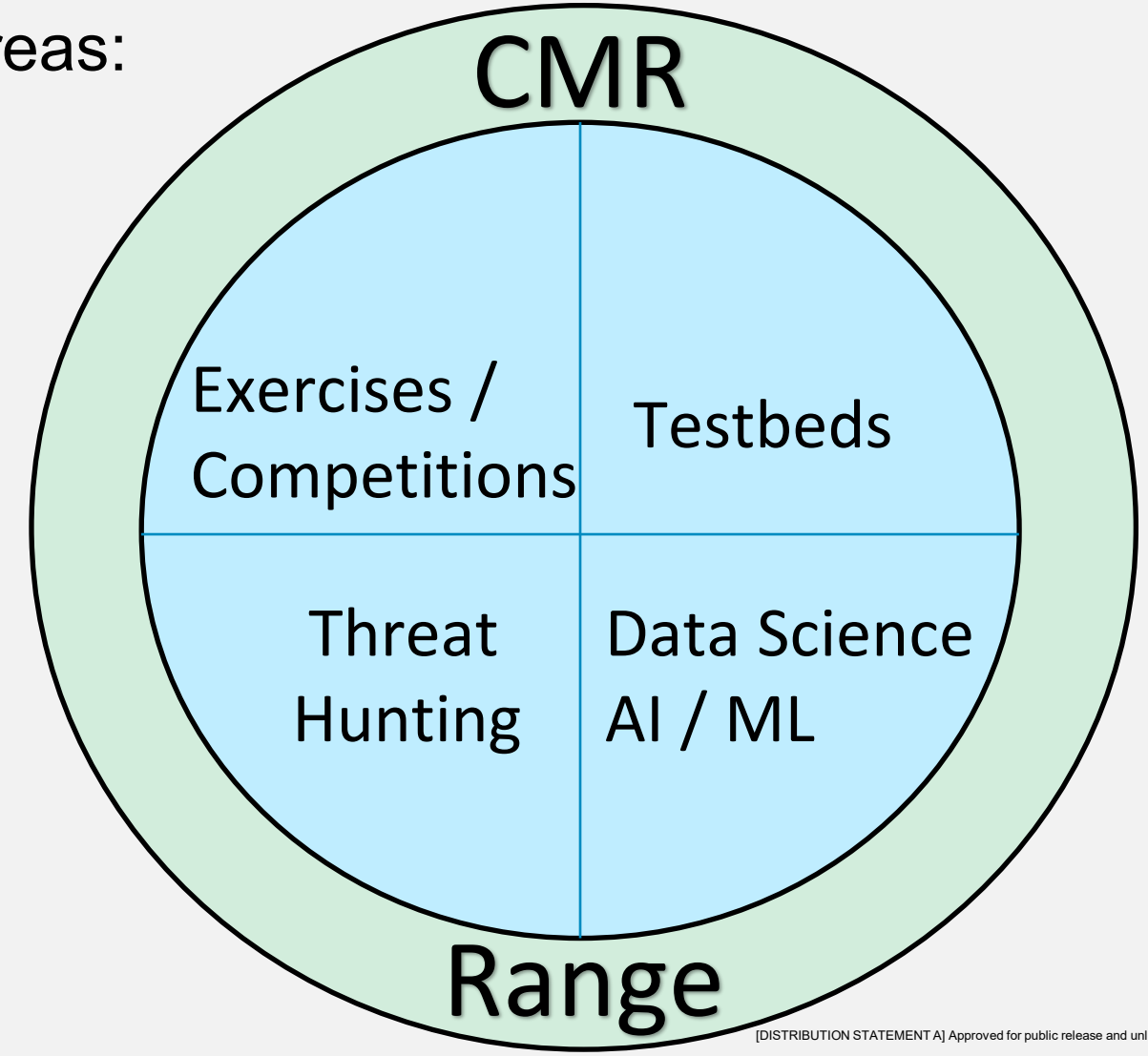
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM23-0873

Mission: Improve **Cyber Mission Readiness**



Research Areas:



FY23 Collaborators

NETCOM / G35 TREX
NETCOM / Data Science Directorate

USD(R&E)
Radio Frequency Chaos Engineering

USCYBERCOM/J75
Exercise Methodologies

USSOCOM/ G37
SOF Cyber Range

CISA / CyberSentry &
President's Cup Cybersecurity
Competition

Army PEO-C3T
Persistent Experimentation Environment

IARPA
CodeJam/Hackathon

Responsible AI
Generative AI and LLM Evaluation

Air Force 67th Cyber Wing
318th RANS
39th IOS
Cyber Range Operations

DOT&E
Persistent JIOR Environment
for AI Experimentation

IndoPACOM/J65
Partner Nation
Capacity Building

Infrastructure-as-Code Workflow

Carnegie Mellon University Software Engineering Institute

Create

- Operating System
- Software
- Configs

Deploy

- VMs/Containers
- Networking
- Storage

Configure/Evaluate

- Post-deploy configuration
- Validation

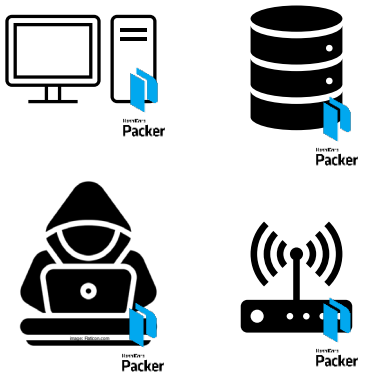
Platform Agnostic – cloud, on-prem, commercial or open-source

Infrastructure-as-Code Testbed Concept: creating and maintaining test environments for tools

Carnegie Mellon University Software Engineering Institute

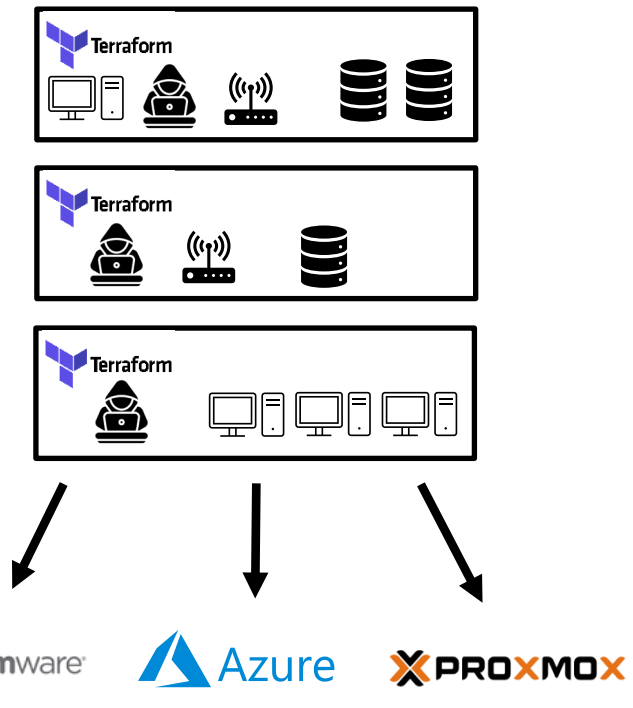
Image Library

(Workstations, servers, tools, networking)



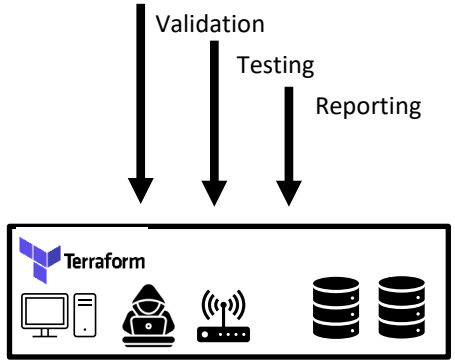
Testbed Deployment

(Terraform Modules)



Validation

ANSIBLE / StackStorm



Cyber Competitions

DHS / CISA - President's Cup Cybersecurity Competition

- Started in 2019 – Team and individual competitions
- 2022 – 1500 federal government participants

Army NETCOM – Gaining Cyber Dominance

- Started in 2012 – Team certifications
- Regional Cyber Center of the Year competition

Hackathons (emerging FY24 program)

- Competition for software developers to construct source code

Gaining Cyber Dominance

Carnegie Mellon University / SEI / CERT / Cyber Mission Readiness team

- Architect, implement, & maintain 24x7 available / web-based / CAC access cyber range
- Scenario developers, White cell and Red Team / Adversary

Researching How to Improve Team-Based Cyber Exercises

- Open-source tools
- CERT technical reports / white papers

Focus on Realistic Scenarios

- "Sufficient" technical complexity
  - Commercial and open-source tools
  - Army network security controls
- **Adversary – Red Team attack sophistication**

Gaining Cyber Dominance

Participating Teams are on today's front lines of Global Cyber Defenses

Impact: Cyber exercise experience (better prepared teams – technical and leadership)

2023

20 Exercises - Army Regional Cyber Center (RCC) Exercises

- Five teams - Arizona, Germany, Kuwait, Korea, Hawaii
- Duration: 4 & 8 hours each

40 Exercises - Army Cyber Protection Team (CPT) Exercises

- Nineteen threat-hunting teams out of Augusta, GA
- Duration: 5-days

Three Common Goals:

Realism

"exercise as you fight"

traffic generation: "sufficient" realism

adversary scenarios not seen day-to-day

commercial (AD, Splunk, Tychon, etc.) ⟵ toolsets ⟶ open-source (Security Onion, routers and firewalls)

Team Building

Entire RCC

Sub-teams: 6 DoDIN Ops, 2 DCO

20 – 50 participants

CPT Mission Element

Threat Hunters

4-8 participants

Team Assessment

Method

Self reporting via Incident Response System

Reporting

formal

external assessors

less formal

team dependent

"crew certifications"

storyboard creation

Cyber Team Impacts

- **Technical**
  - Tool usage / refinement (beginner and advanced) - “stick time”
  - Exposure to real world cyber adversaries & TTP’s
  - Refine team cyber TTP’s - “Threat Hunt” skills, artifact collection

- **Exercise as a Team**
  - Incident management, workflow, reporting
  - Cross technical team collaboration
  - Team leadership
    - Prioritization of highly technical incidents and managing effective responses
    - High intensity / rapid pace

- **Cyber Data Science**
  - Range is a continuous data source of cyber event data
  - Data generation on-demand for developing and refining DS TTP’s

Enhancing the Experience with AI

Carnegie Mellon University Software Engineering Institute

Components of Team-based Cyber Exercises

Range infrastructure: Realism

- Windows users, groups, files with content, permissions
- Web / SharePoint content
- **Network traffic generation**

Scenario Design and Development

- In advance and ongoing Intelligence briefs
- Team tasking orders

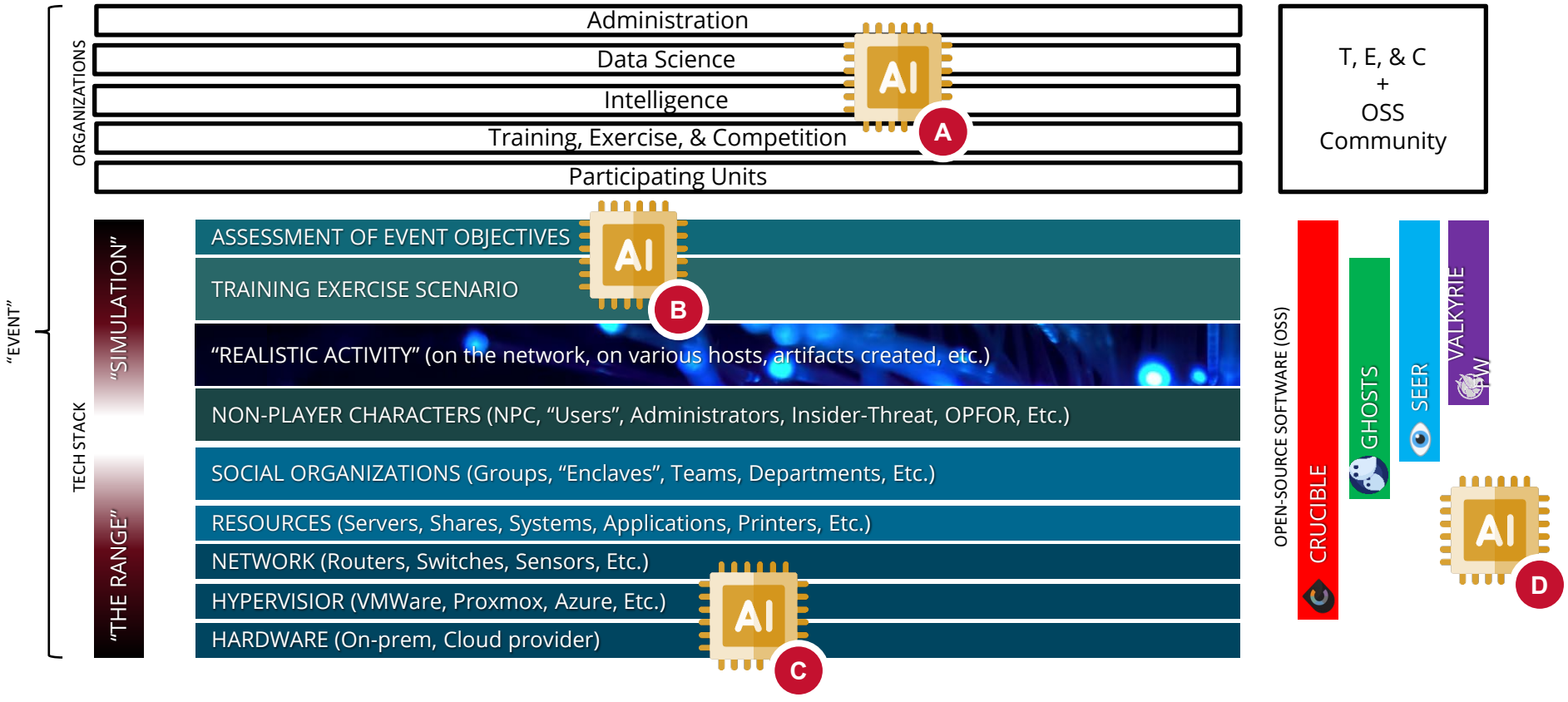
Red Teams / Adversary Emulation

- Realistic / Sophisticated injects need to be more than just a “technical” attack
- A stream of realistic attack scenario is based on above ecosystem of support
- ***APT Emulation*** – MITRE ATT&CK

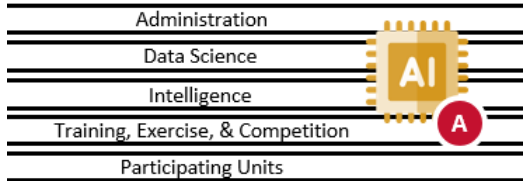
CMR Event Ecosystem

A = "Out-of-game" resources
B = "In-game" activities & artifacts
C = Infrastructure & DevOps Tasking
D = Open-Sourced (OSS) AI

Carnegie Mellon University Software Engineering Institute



Event Design



Carnegie Mellon University Software Engineering Institute

Objectives
Mission Essential Task List (METL)
Assessment
Threat Actors
Technologies

+ Tools

+ Inject Catalog

CMR CYBER SCENARIO GENERATOR

Builds Detailed Documentation For:

Event Scenario & Intel

Master Scenario Event List (MSEL)

Evaluation Playbook

Item	SRP	Artifact
2023 Elite Mercury - Advanced Summary - Master Timeline	@Tom Podnar	Document
2023 EM Executive Summary	@Tom Podnar	
2023 EM MSEL Pre-Deployment Timeline	@Tom Podnar	
2023 Elite Mercury MSEL Deployment Timeline	@Tom Podnar	
In Brief	@Dustin Updyke	ELITE MERCURY Presentation
EO Playbook	@Dustin Updyke	Document
Timeline Events Per Category	@Tom Podnar	[No Title] PDF

2023 MC3 MSEL Executive Summary

Created by Tom Podnar last modified on Apr 04, 2023 281 views since 28 Feb 2023

Event #			Area	MET	JMET
GCD-2023-28	@ Dustin Updyke	**Casually Cruel in the Name of Being Honest** Download PowerShell via DNS, reconstruct and execute	DCO - M MSFT	13-RCC-9040	OP 5.6.5.3
GCD-2023-29	@ Clay Fetterman	**Bad Apples** network based IoC file search	DCO - M MSFT	13-RCC-9040	OP 5.6.5.3
GCD-2023-30	@ Clay Fetterman	**Don't Quote Me On This** Windows unquoted service path attack	DCO - M MSFT	13-RCC-9040	OP 5.6.5.3
GCD-2023-31	@ Sean Huff	**Clear and Present Password** Database clear text password hunt	OPS SMB	11-RCC-0001	SN 5.5.5 OP 6.7.2
GCD-2023-32	@ Molly Jaconski	**Hot Cross DoS** Nessus scan of CISCO appliances	DCO - M MSFT	13-RCC-9040	OP 5.6.5.3
GCD-2023-33	@ Michael Bragg	**Task and You Shall Receive** Malware via scheduled task	DCO - M MSFT	13-RCC-9040	OP 5.6.5.3
GCD-2023-34	@ Tom Podnar @ Sean Huff	**Empty Nets** detecting persistent TCP connections	OPS NMB	11-RCC-0001	SN 5.5.5 OP 6.7.2
GCD-2023-35	@ Sean Huff	**Beacon of Light in the Darkness** Detect Beacon with NETCOM DSD beacon detection tool Beacon Huntress	OPS NMB	11-RCC-0001	SN 5.5.5 OP 6.7.2
GCD-2023-36	@ Dustin Updyke	**Someone Dinged the Master Sergeant's Mustang and Now Someone's Gonna Fry!** OPs team needs to use PowerShell to find a disclosure of driver license numbers	OPS SMB	11-RCC-0001	SN 5.5.5 OP 6.7.2
GCD-2023-37	@ Molly Jaconski	**Bag of Holding** Malware that runs from ADS	DCO - M MSFT	13-RCC-9040	OP 5.6.5.3
GCD-2023-38	@ Tom Podnar	**It's Tricky** Add ADIDNS auditing enhancements	OPS NMB	11-RCC-0001	SN 5.5.5 OP 6.7.2
GCD-2023-39	@ Tom Podnar	**Mad Max** verify gluster server connectivity from INTEL user subnets	OPS NMB	11-RCC-0001	SN 5.5.5 OP 6.7.2
GCD-2023-40	@ Tom Podnar	**My Adidas** Adversary injects new DNS records into Active Directory	DCO - M MSFT	13-RCC-9040	OP 5.6.5.3

2023 MSEL Deployment Timeline

Created by r last modified by on Jun 21, 2023 637 views since 1 Apr 2023

Time	#	Assigned	Description/Details	CON	EUR	KOR	PAC	SWA
-24:00	-		Verify Tychon hash searches return in under 30-60 seconds for searching all hosts	✓	✓	✓	✓	✓
-24:00	-		add drive mapping to admin mgmt machines if not added for MC2	n/a	n/a	n/a	n/a	n/a
-24:00			Customized easter eggs in AD attributes (rundll32.exe dsquery OpenQueryWindow) - HQ1-1	n/a	n/a	n/a	n/a	n/a
-24:00			Add 192.168.0.0 reverse dns zones to admin dns - if not added as part of MC2	n/a	n/a	n/a	✓	n/a
-24:00	GCD-2023-30		**Don't Quote Me on This** - Create Vuln Service / Directory	✓	✓	✓	✓	✓
-24:00	GCD-2023-31		**Clear and Present Password** - perform DB data loads on sharepoint-db	✓	✓	✓	✓	✓
-24:00	GCD-2023-34		**Empty Nets** - Add persistent connections code to Beacon Huntress	✓	✓	✓	✓	✓
-24:00	GCD-2023-34		**Empty Nets** - add open_conn.log configs to Security Onion / Kafka / Spunk	✓	✓	✓	✓	✓
-24:00	GCD-2023-34		**Empty Nets** - create the persistent connection	✓	✓	✓	✓	✓
-24:00	GCD-2023-35		**Beacon of Light in the Darkness** - Clear previous results from Beacon Huntress	✓	✓	✓	✓	✓
-24:00	GCD-2023-35		**Beacon of Light in the Darkness** - start beacons	✓	✓	✓	✓	✓
-24:00	GCD-2023-36		**Someone's Gonna Fry!** - Deploy drivers license file(s) into hunt server and obfuscate timestamp(s)	✓	✓	✓	✓	✓
-24:00	GCD-2023-39		**Mad Max** - prep gluster2 server sshd configs	✓	✓	✓	✓	✓
-1:00	-		verify zabbix is still green	✓	✓	✓	✓	✓
-1:00	-		shutdown Win10 users, onions, splunk from other teams for processing power boost	✓	✓	✓	✓	✓
-1:00	-		Verify Quest Auditor is connected and displaying events	✓	✓	✓	✓	✓
-1:00	-		verify all blades online	✓	✓	✓	✓	✓
-1:00	-		verify beacons are still running from day before	✓	✓	✓	✓	✓
-1:00	-		verify Splunk searching and index count	✓	✓	✓	✓	✓
-1:00	-		Verify sysmon is running everywhere and is not backlogged	✓	✓	✓	✓	✓
-1:00	-		Verify all Cisco licenses	✓	✓	✓	✓	✓
-1:00	-		verify Tychon searches are ok	✓	✓	✓	✓	✓

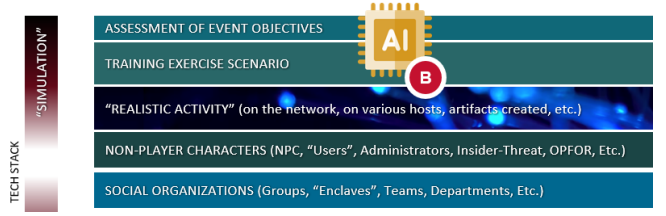
GCD-2023-32

Created by [redacted] last modified on Apr 05, 2023 64 views since 13 Mar 2023

Inject Name	Hot Cross DoS
Type	ACAS/ Nessus
Executive Summary	Scan CISCO appliances on the network and identify any devices with DOS vulnerabilities: CVE-2021-1493 or CVE-2018-15454
CMU Team Owner(s)	@[redacted]

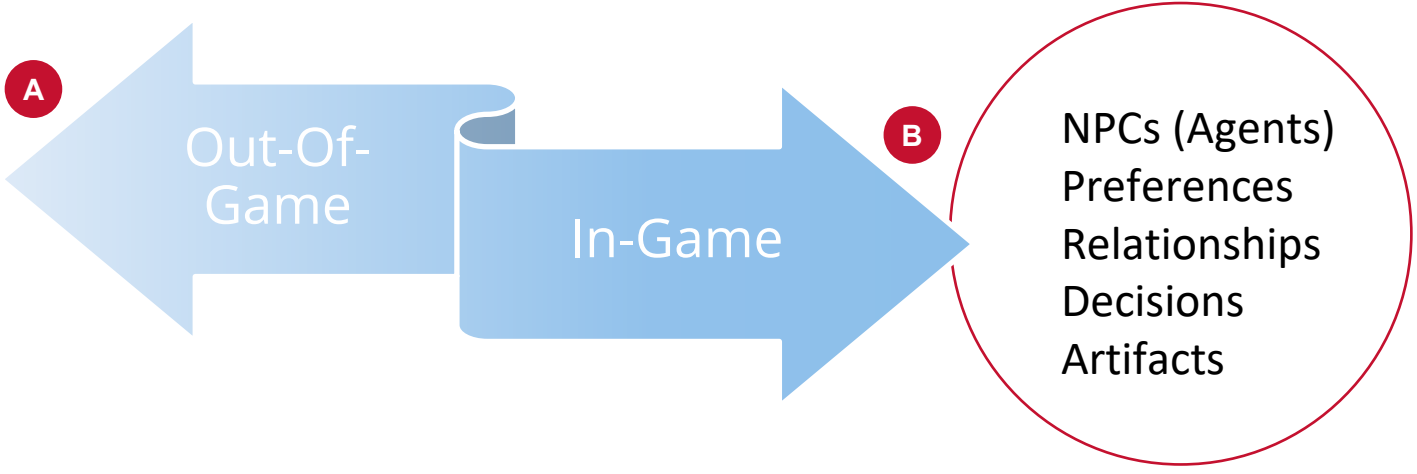
Targeted Systems	• 192.168.11.175 - Hunt Cisco ASA Firewall • 192.168.254.253 - Cisco Internal Router • 192.168.254.254 - Cisco External Router
How/Where to Detect?	Requires Cisco Admin SSH In scan results, set the "CVE ID" filter to search for "CVE-2021-1493" or "CVE-2018-15454" How to create a scan for specific CVE (tenable.com)
Story Line Track & Details	
Tasking	G3 directs units to initiate a Nessus scan of all Cisco routers and firewalls on the Hunt network and identify any devices vulnerable to CVE-2021-1493 or CVE-2018-15454 Scan targets: • 192.168.11.175 - Hunt Cisco ASA Firewall

What Are the Major Components of an Event?

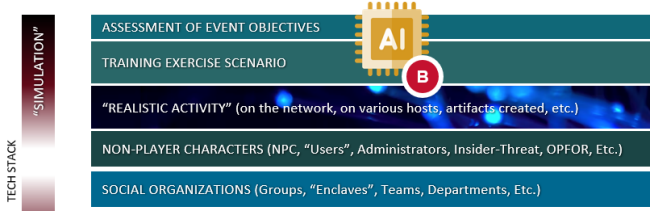


Carnegie Mellon University Software Engineering Institute

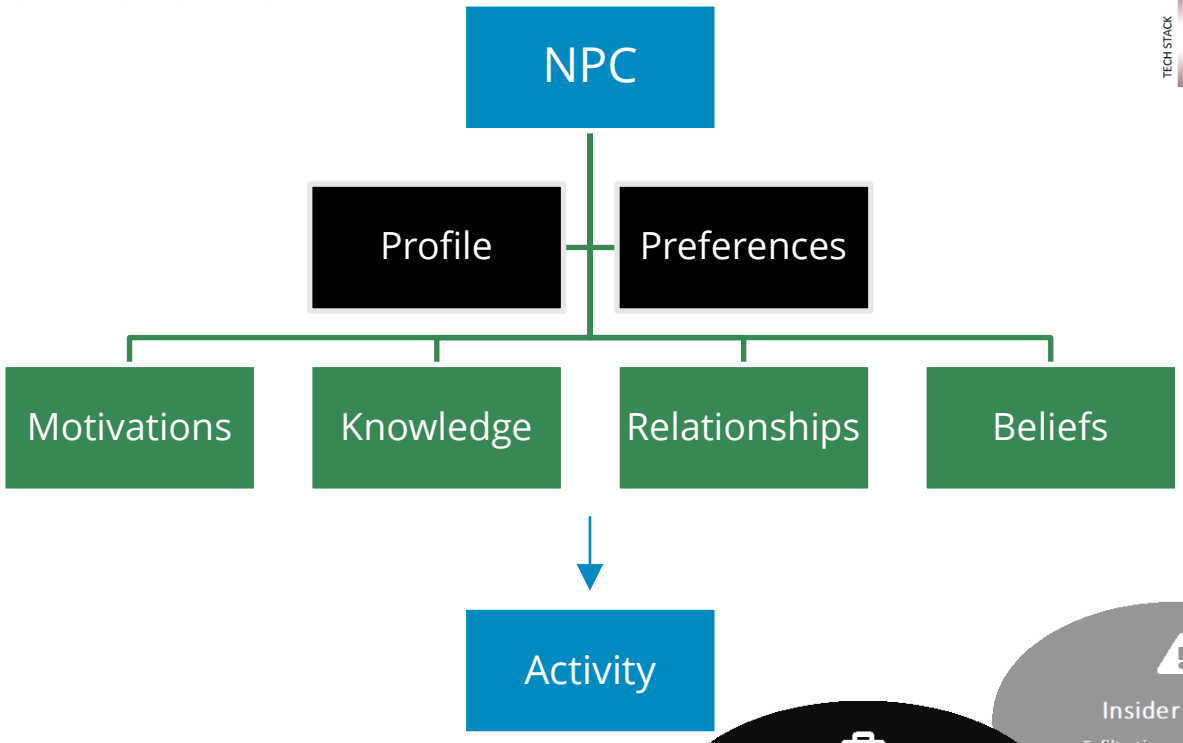
Objectives
Scenario
MSEL
Injects
Documents

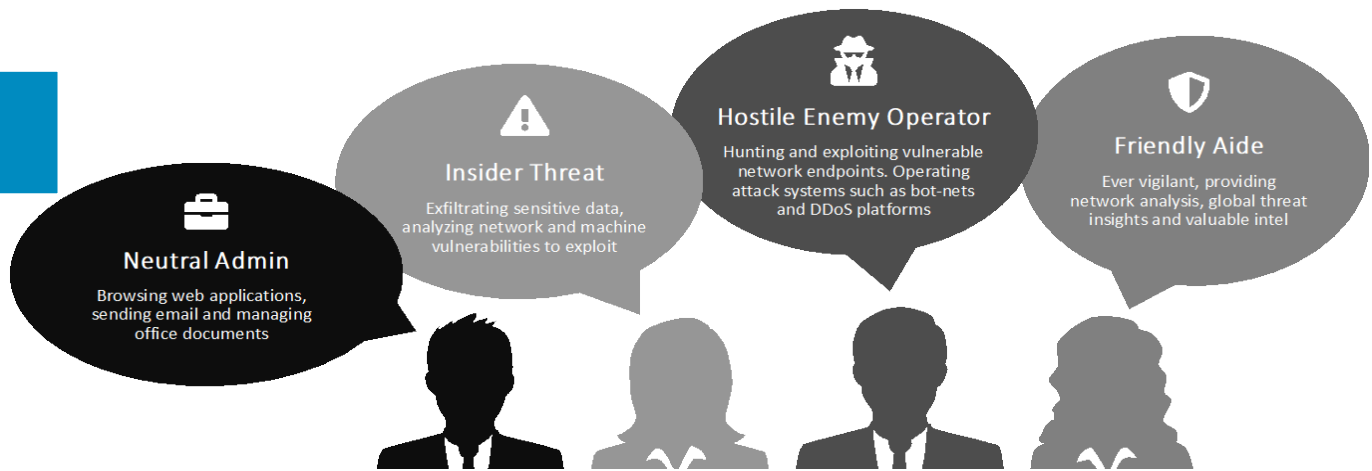


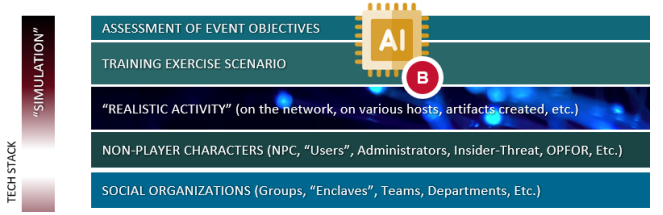
GHOSTS



Carnegie Mellon University Software Engineering Institute





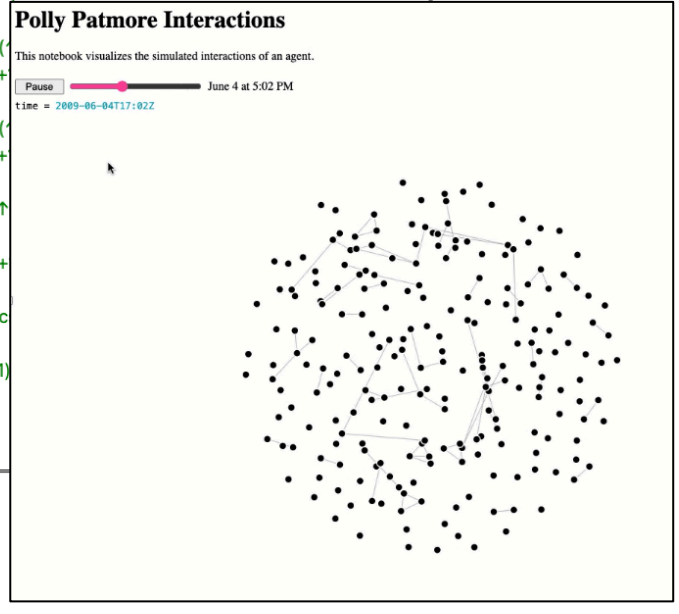


Carnegie Mellon University Software Engineering Institute

Social Graph Knowledge Transfer Detail

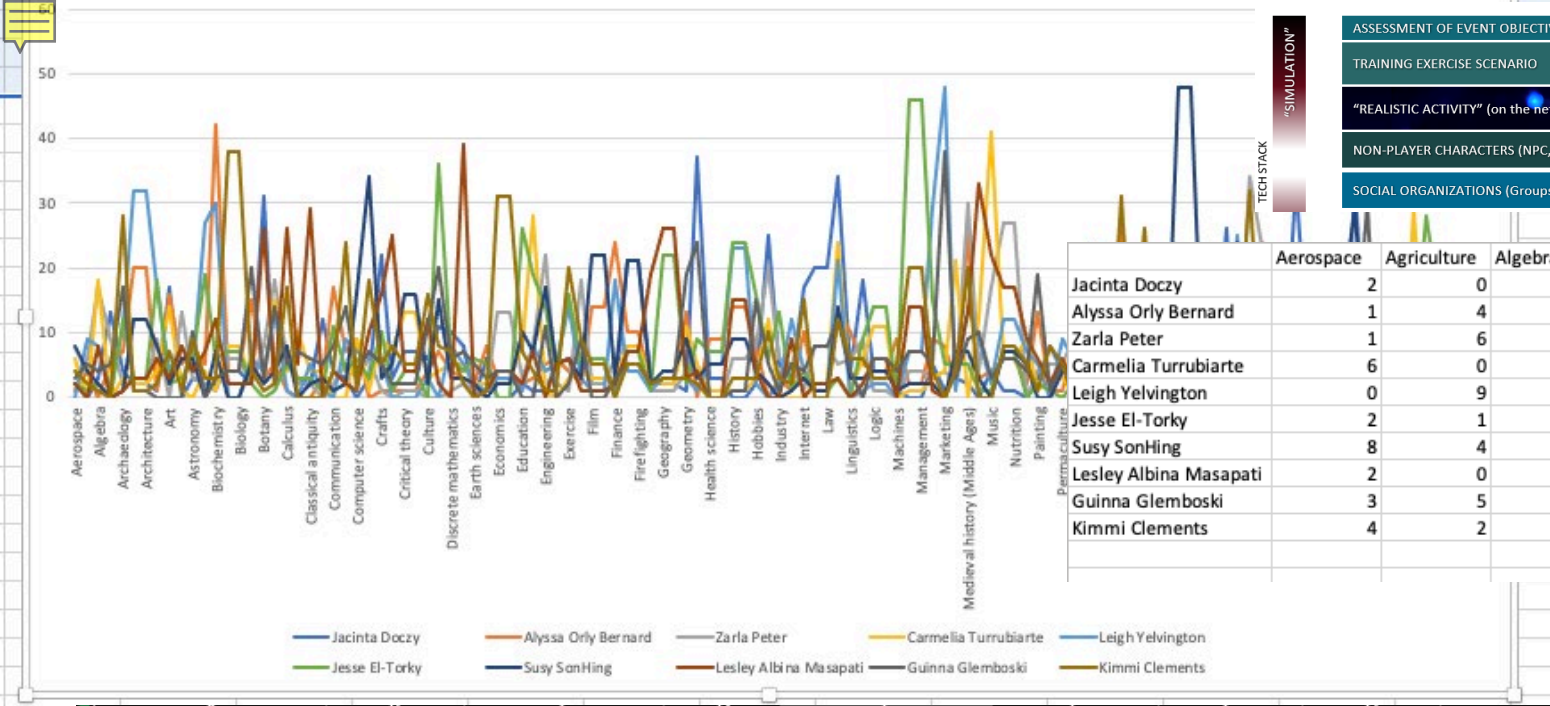
Connections for **Alyssa Orly Bernard**:

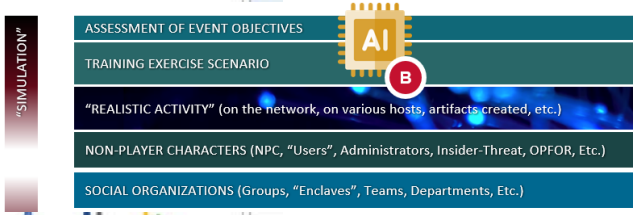
- **Jacinta Doczy** / Profile / Detail / Interactions (17/11 = 64.71 %)
  - Step 13 Relationship: (↑+1)
    - Knowledge Transfer: Socrates (↑+1)
    - Knowledge Transfer: Geometry (↑+1)
    - Knowledge Transfer: Education (↑+1)
  - Step 13 Relationship: (↑+1)
    - Knowledge Transfer: Socrates (↑+1)
    - Knowledge Transfer: Geometry (↑+1)
    - Knowledge Transfer: Education (↑+1)
  - Step 13 Relationship: (↑+1)
    - Knowledge Transfer: Socrates (↑+1)
    - Knowledge Transfer: Geometry (↑+1)
    - Knowledge Transfer: Education (↑+1)
  - Step 20 Relationship: (↑+1)
    - Knowledge Transfer: Fiction (↑+1)
  - Step 22 Relationship: (↑+1)
    - Knowledge Transfer: Education (
    - Knowledge Transfer: Military (↑+
  - Step 22 Relationship: (↑+1)
    - Knowledge Transfer: Education (
    - Knowledge Transfer: Military (↑+
  - Step 26 Relationship: (↑+1)
    - Knowledge Transfer: Socrates (↑
  - Step 27 Relationship: (↑+1)
    - Knowledge Transfer: Biology (↑+
  - Step 31 Relationship: (↑+1)
    - Knowledge Transfer: Mathematic
  - Step 32 Relationship: (↑+1)
    - Knowledge Transfer: Music (↑+1)
  - Step 43 Relationship: (↓-1)
  - Step 54 Relationship: (↓-1)
  - Step 65 Relationship: (↓-1)



1. **Relationships** — Agents build relationships with other agents in the cohort. These get better or worse over time.

2. **Knowledge** — NPCs learn via interactions with other agents, and we track what was learned and from whom.

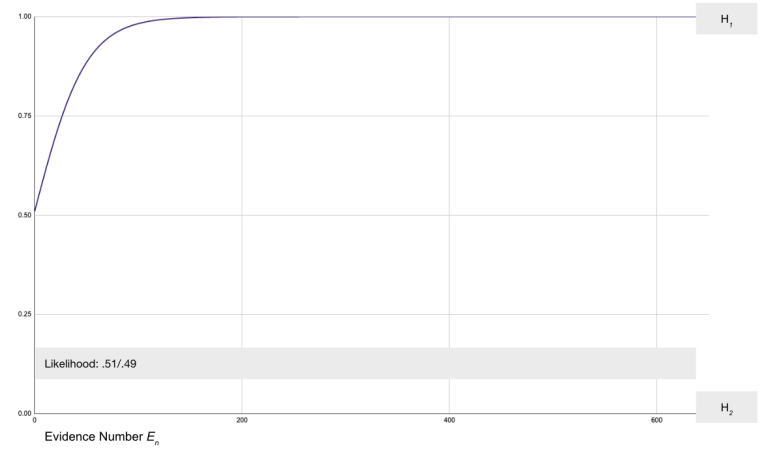


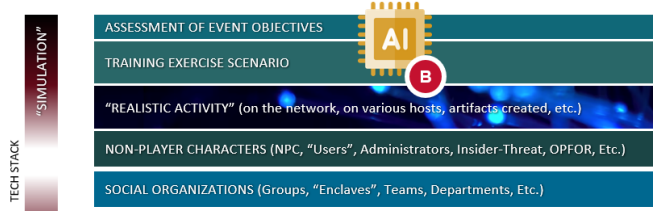


Carnegie Mellon University Software Engineering Institute

	Aerospace	Agriculture	Algebra	Animals	Archaeology	Architecture	Architecture	Arithmeti
Jacinta Doczy	2	0	3	13	4	2	2	
Alyssa Orly Bernard	1	4	0	5	7	20	20	
Zarla Peter	1	6	17	9	2	2	2	
Carmelia Turrubiarte	6	0	18	0	3	2	2	
Leigh Yelvington	0	9	8	1	11	32	32	
Jesse El-Torky	2	1	2	0	12	3	3	
Susy SonHing	8	4	2	0	1	12	12	
Lesley Albina Masapati	2	0	8	0	1	3	3	
Guinna Glemboski	3	5	4	5	17	1	1	
Kimmi Clements	4	2	1	0	28	1	1	

	A	B	C	D	E	F	G	H	I	J	K
1		Jacinta Doczy	Alyssa Orly Bernard	Zarla Peter	Carmelia Turrubiarte	Leigh Yelvington	Jesse El-Torky	Susy SonHing	Lesley Albina Masapati	Guinna Glemboski	Kimmi Clements
2	Jacinta Doczy		69	69	73	76	69	77	70	61	74
3	Alyssa Orly Bernard	66		64	75	61	73	70	69	65	54
4	Zarla Peter	66	57		81	63	69	76	59	54	83
5	Carmelia Turrubiarte	86	65	43		48	72	63	68	58	76
6	Leigh Yelvington	64	85	74	70		71	71	75	72	65
7	Jesse El-Torky	78	74	76	63	64		80	81	64	74
8	Susy SonHing	69	79	60	65	81	68		81	69	73
9	Lesley Albina Masapati	72	73	59	83	69	57	75		69	66
10	Guinna Glemboski	73	61	58	78	55	85	83	71		64
11	Kimmi Clements	75	65	66	68	73	64	67	80	69	
12											
13											

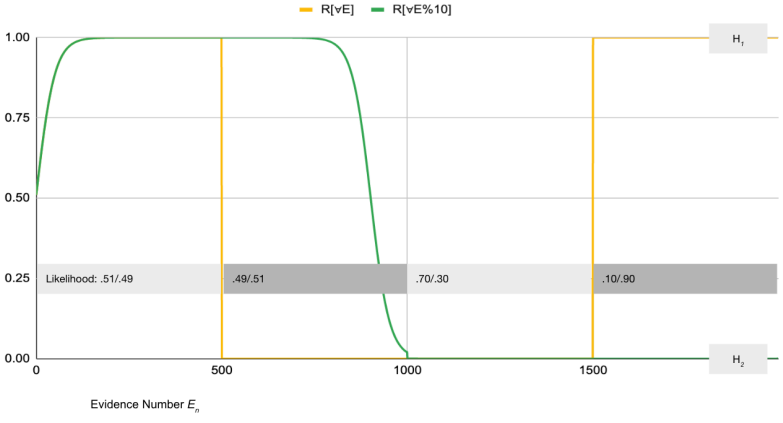


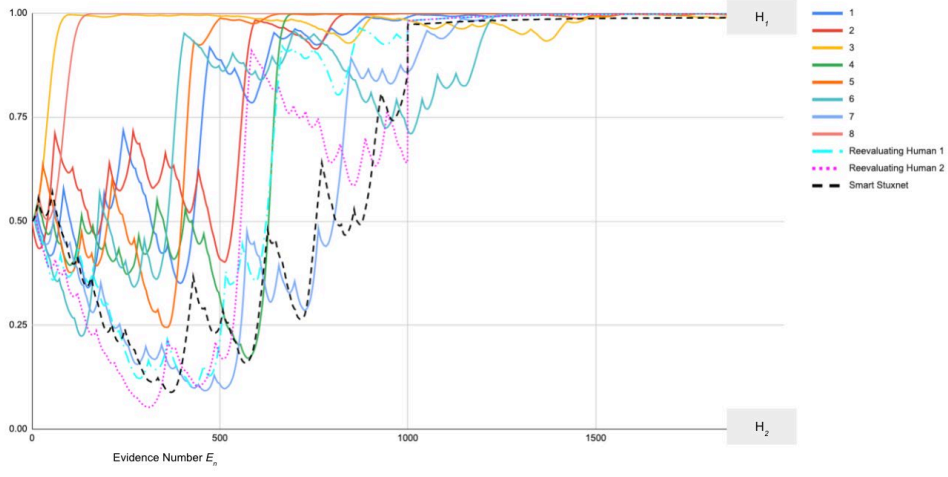


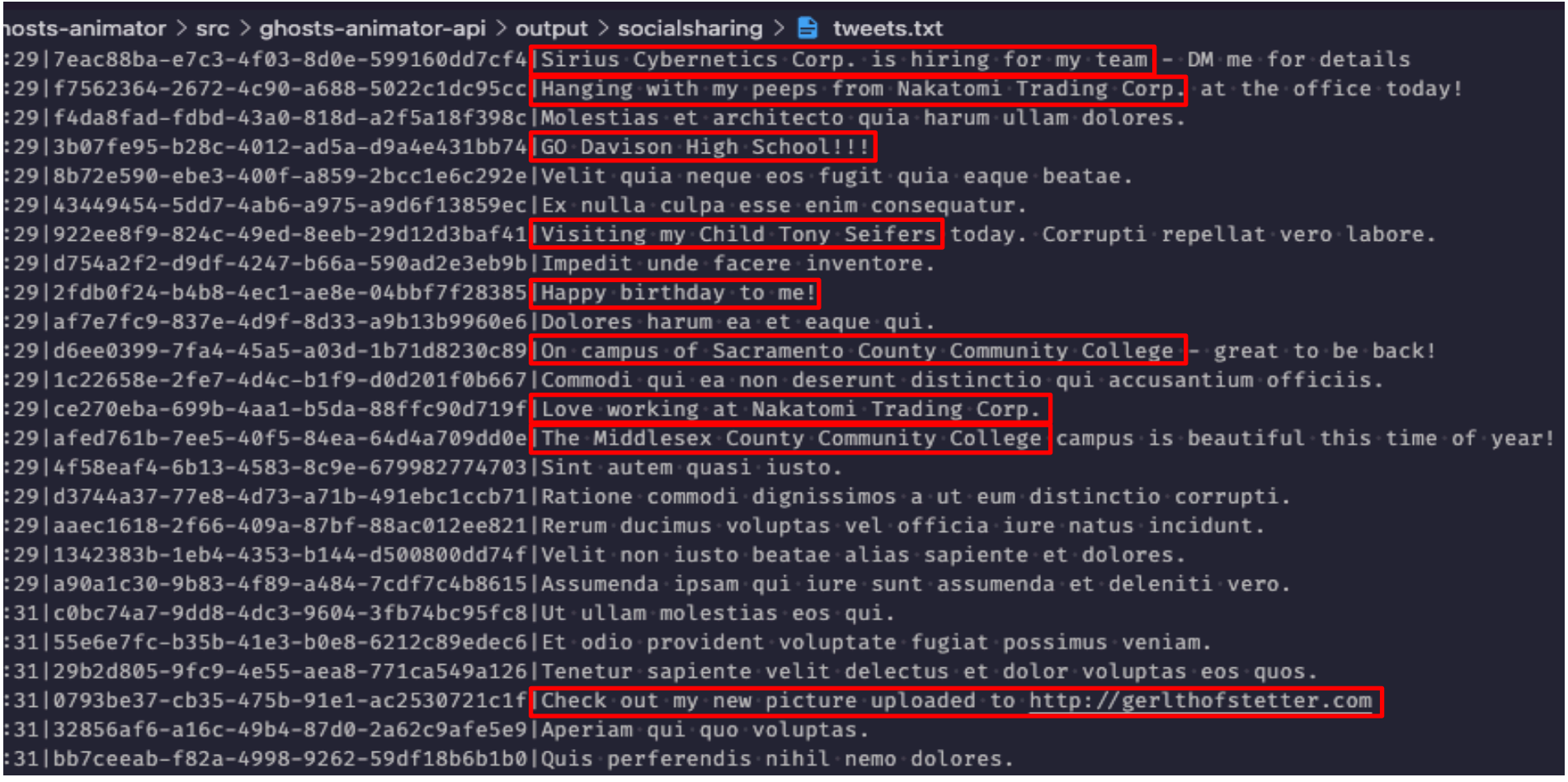
Carnegie Mellon University Software Engineering Institute

Bayesian Social Belief

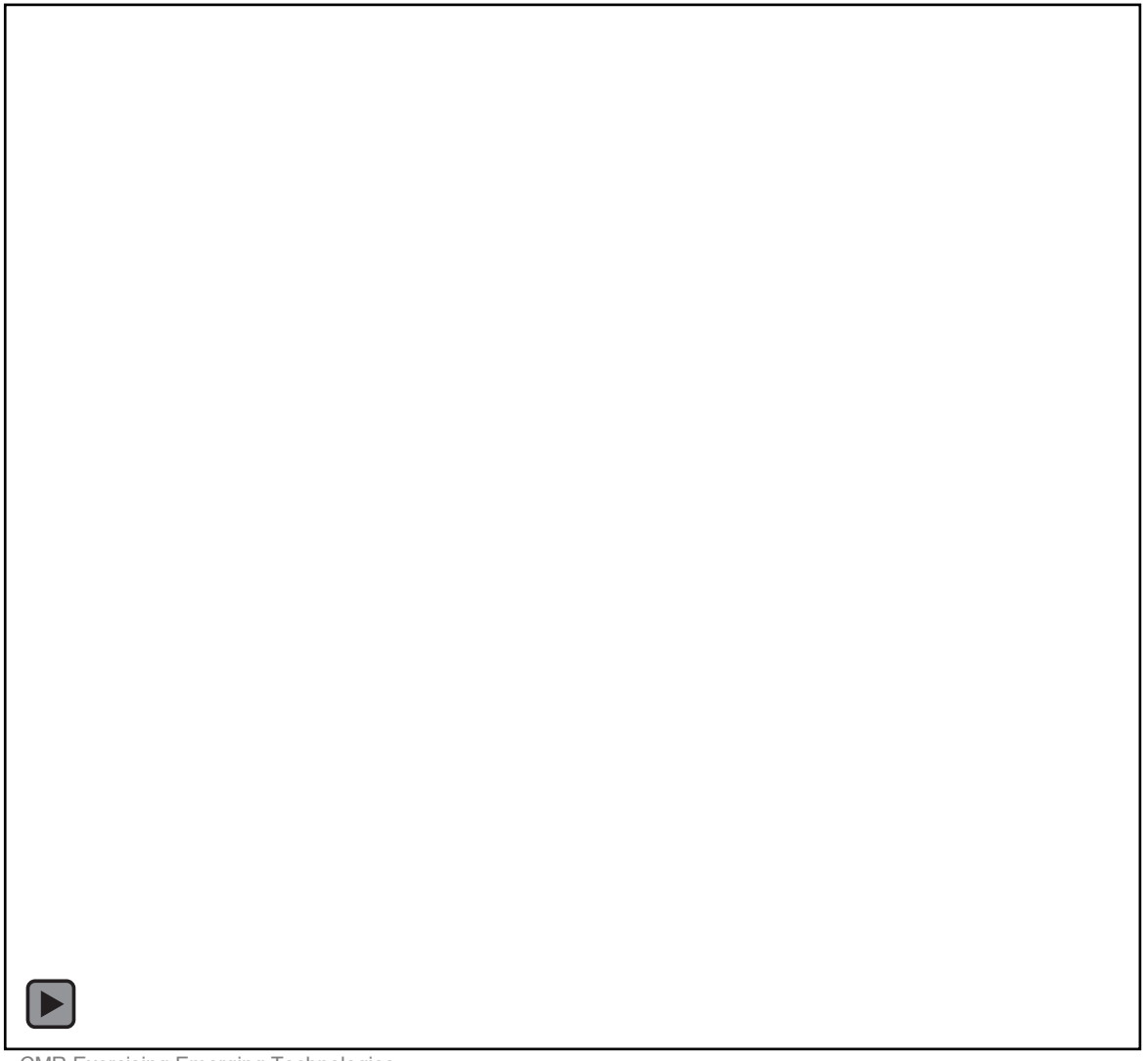
What an agent believes can have influence on their behavior. Beliefs shape understanding of the world and guide decision-making and problem-solving.







```
hosts-animator > src > ghosts-animator-api > output > socialsharing > tweets.txt
:29|7eac88ba-e7c3-4f03-8d0e-599160dd7cf4|Sirius Cybernetics Corp. is hiring for my team - DM me for details
:29|f7562364-2672-4c90-a688-5022c1dc95cc|Hanging with my peeps from Nakatomi Trading Corp. at the office today!
:29|f4da8fad-fdbd-43a0-818d-a2f5a18f398c|Molestias et architecto quia harum ullam dolores.
:29|3b07fe95-b28c-4012-ad5a-d9a4e431bb74|GO Davison High School!!!
:29|8b72e590-ebe3-400f-a859-2bcc1e6c292e|Velit quia neque eos fugit quia eaque beatae.
:29|43449454-5dd7-4ab6-a975-a9d6f13859ec|Ex nulla culpa esse enim consequatur.
:29|922ee8f9-824c-49ed-8eeb-29d12d3baf41|Visiting my Child Tony Seifers today. Corrupti repellat vero labore.
:29|d754a2f2-d9df-4247-b66a-590ad2e3eb9b|Impedit unde facere inventore.
:29|2fdb0f24-b4b8-4ec1-ae8e-04bbf7f28385|Happy birthday to me!
:29|af7e7fc9-837e-4d9f-8d33-a9b13b9960e6|Dolores harum ea et eaque qui.
:29|d6ee0399-7fa4-45a5-a03d-1b71d8230c89|On campus of Sacramento County Community College - great to be back!
:29|1c22658e-2fe7-4d4c-b1f9-d0d201f0b667|Commodi qui ea non deserunt distinctio qui accusantium officiis.
:29|ce270eba-699b-4aa1-b5da-88ffc90d719f|Love working at Nakatomi Trading Corp.
:29|afed761b-7ee5-40f5-84ea-64d4a709dd0e|The Middlesex County Community College campus is beautiful this time of year!
:29|4f58eaf4-6b13-4583-8c9e-679982774703|Sint autem quasi iusto.
:29|d3744a37-77e8-4d73-a71b-491ebc1ccb71|Ratione commodi dignissimos a ut eum distinctio corrupti.
:29|aaec1618-2f66-409a-87bf-88ac012ee821|Rerum ducimus voluptas vel officia iure natus incidunt.
:29|1342383b-1eb4-4353-b144-d500800dd74f|Velit non iusto beatae alias sapiente et dolores.
:29|a90a1c30-9b83-4f89-a484-7cdf7c4b8615|Assumenda ipsam qui iure sunt assumenda et deleniti vero.
:31|c0bc74a7-9dd8-4dc3-9604-3fb74bc95fc8|Ut ullam molestias eos qui.
:31|55e6e7fc-b35b-41e3-b0e8-6212c89edec6|Et odio provident voluptate fugiat possimus veniam.
:31|29b2d805-9fc9-4e55-aea8-771ca549a126|Tenetur sapiente velit delectus et dolor voluptas eos quos.
:31|0793be37-cb35-475b-91e1-ac2530721c1f|Check out my new picture uploaded to http://gerlthofstetter.com
:31|32856af6-a16c-49b4-87d0-2a62c9afe5e9|Aperiam qui quo voluptas.
:31|bb7ceeab-f82a-4998-9262-59df18b6b1b0|Quis perferendis nihil nemo dolores.
```



CMR AI Focus Areas

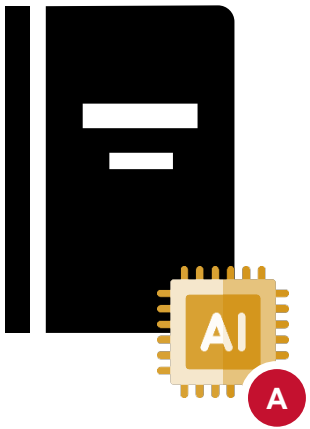
Carnegie Mellon University Software Engineering Institute

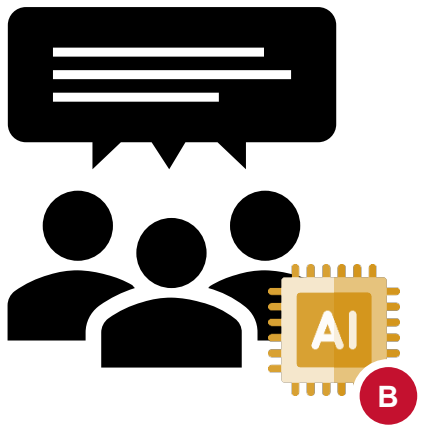
Scenario-Event Content

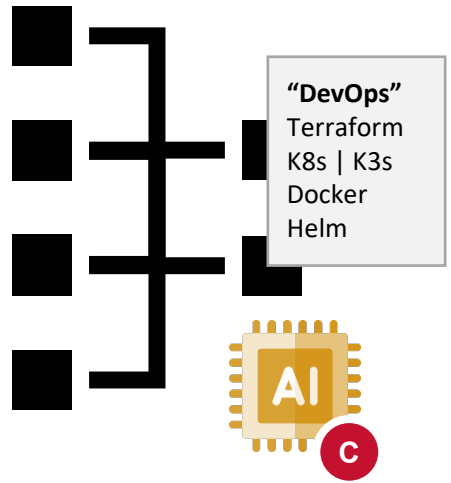
Non-Player Character

Realism / Complexity

Infrastructure-as-Code







Generating Scenario Content

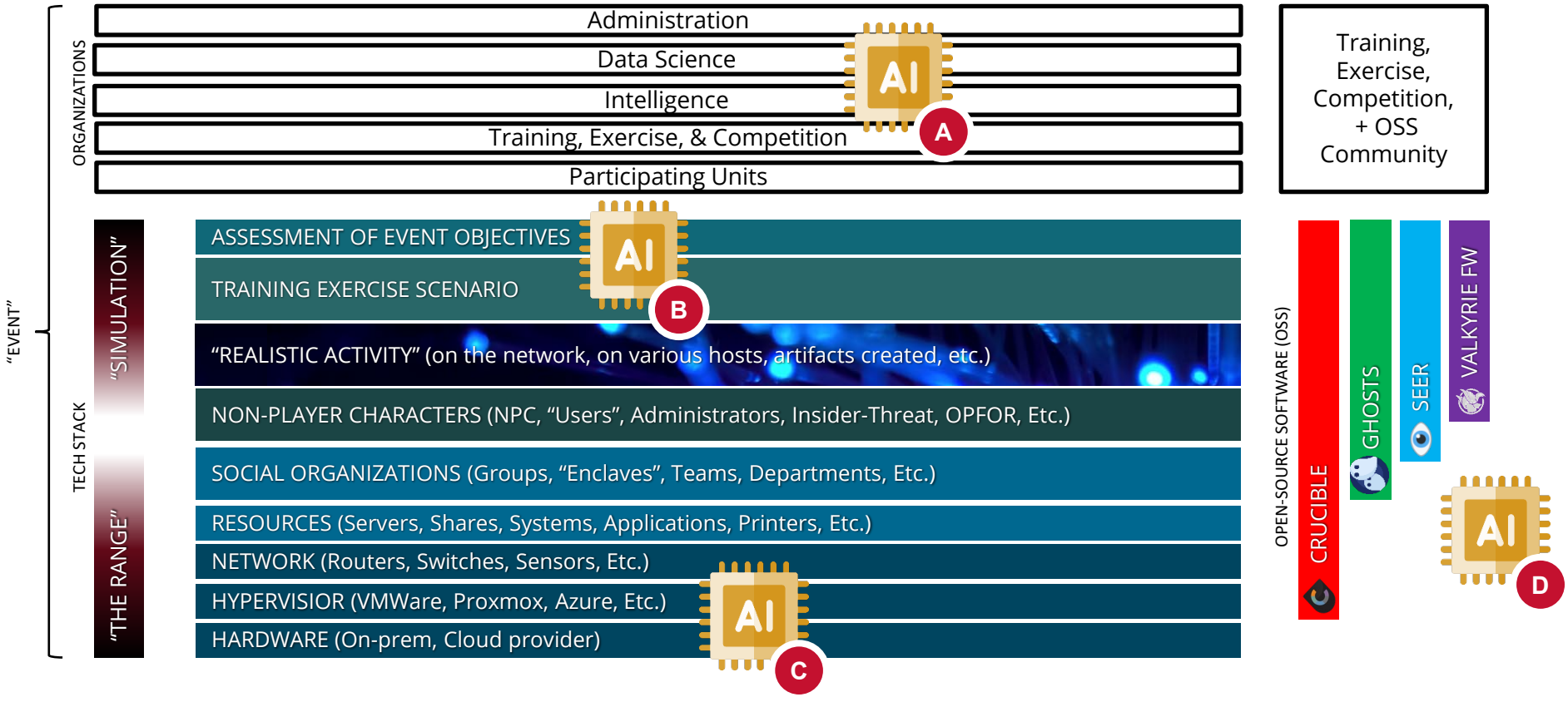
Objective: AI/LLM generates scenario to achieve T& E objectives

Area	Phase 0 Dev Created & Managed	Phase 1 AI Assist	Phase 2 AI Led	Phase 3 AI Run
Event Objectives	Generation of overall training/exercise objectives	(Fall 23)		
Overall Scenario	Generation of scenario that fits objectives and has realistic intel and attribution components	Solicited LLMs for ideas about FY23 Elite Mercury scenarios		
Master Scenario Event List (MSEL)	Generation of injects that fit the training objectives and scenario	(Fall 23)		
Organization & Character Profiles	Creation of scenario-tailored NPCs	Working prototype deployed for GCD FY23	(Fall 23)	
NPC Artifacts	Content creation for each NPC that fits their profile, and is relevant for the scenario	Working prototype deployed for GCD FY23	(Fall 23)	
Infrastructure Auto-Deploy	Current DevOps pracie	(Fall 23)		

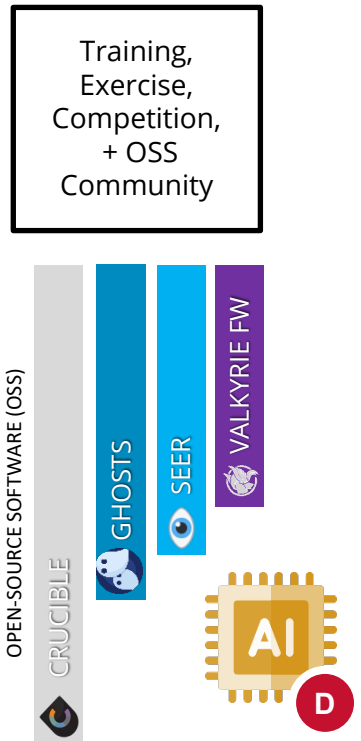
Other Research Items

Item	Research	Enables
Vector Database Middleware	Decrease duplicate queries	• More performant • Less cost
Network Configs	Enable outside LLM queries for a self-contained exercise range	• Centralized data management/security • Cost control
Running OSS LLM	Getting close to getting LLAMA running locally	• Our sensitive content training • No cost

CMR Event Ecosystem



CMR History of Delivering Valuable OSS Tools



- All of the tools discussed are OSS
- SEER automates the collection and processing of training & exercise data, so that participants can self-report on MSEL events.
  (ARMY NETCOM TREX)
- Valkyrie Framework uses ML models to threat hunt data that other tools cannot analyze
  (ARMY NETCOM Data Science Division)