

Cyber Range Research and Development

MAY 11, 2023

John Yarger



Copyright 2023 Carnegie Mellon University.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM23-0477

Agenda

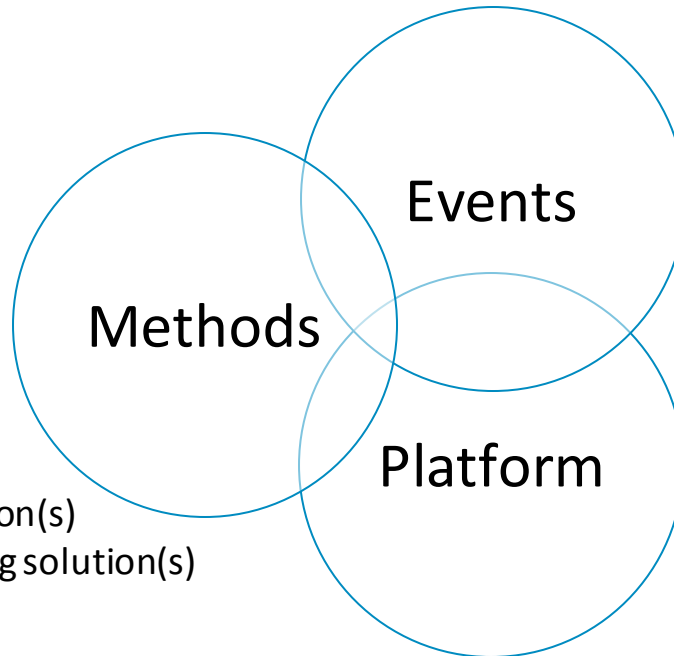
- Big Picture
- Our Three-Month Target

Cyber Range Research and Development

Big Picture

Focus

The **research and development of cyber-range solutions to operational-readiness challenges.**



Our Role

Trusted advisor:

- Framing challenge(s)
- Analyzing potential solution(s)
- Prototyping and exercising solution(s)
- Transitioning solution(s)

Decrease Costs

- Automate Creation

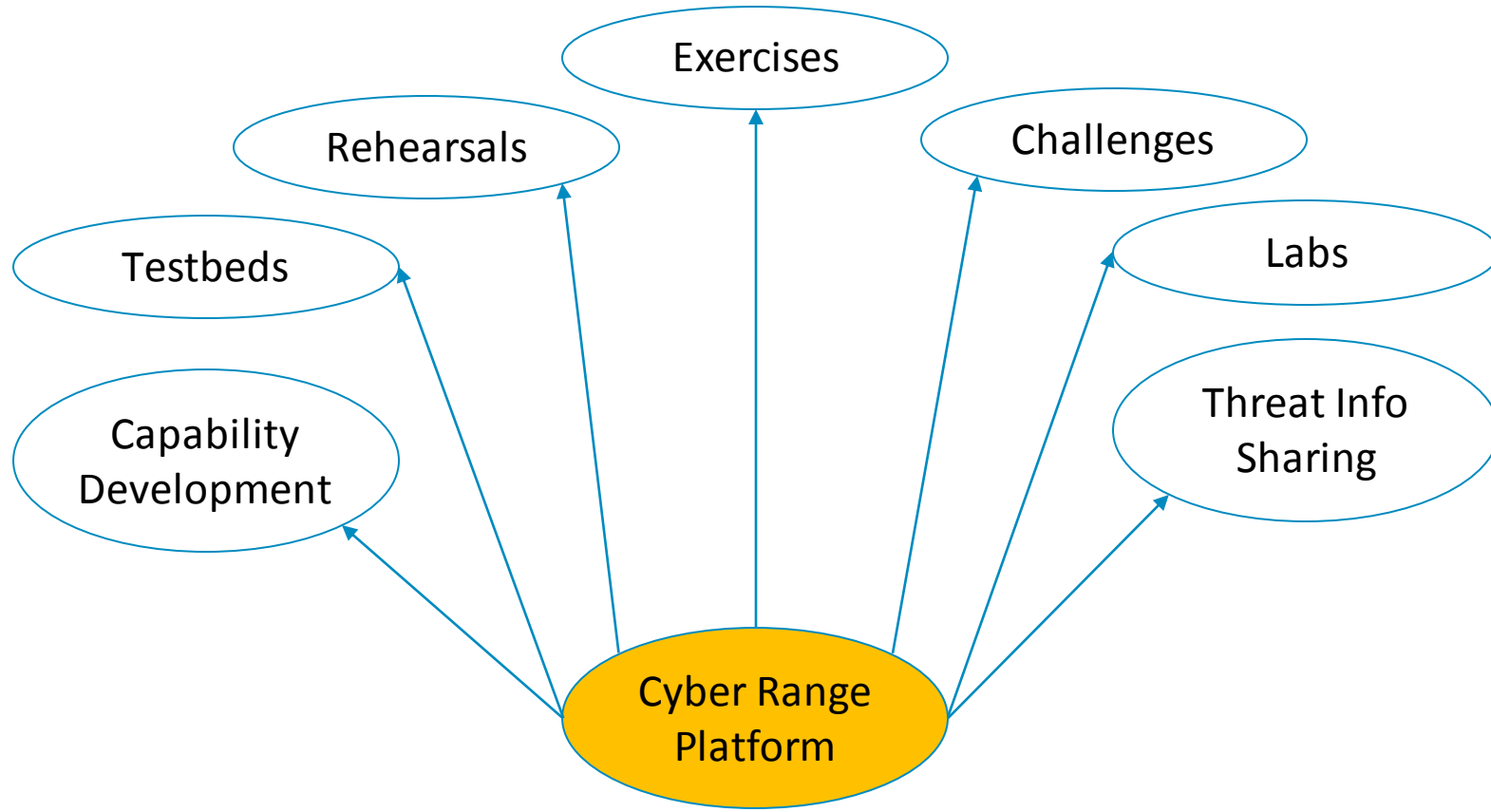
Increase Quality

- Better experiences

Increase Availability

- Maximize Access

Scope of Impact



Challenges



Achievable Using:

Modular Open System Approach
API-First Design

Agile / DevSecOps

Open Source Software

Containerization

Everything as Code

Microservice Architecture

Hypervisor Agnostic

Cyber Range Research and Development

Our Three-Month Target

LLM / Generative AI

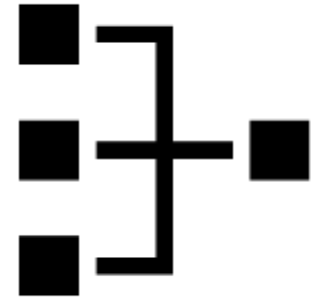
Scenario-Event Content



Non-Player Character
Realism / Complexity



Infrastructure-as-Code





Generating Scenario Content

- **Objective:** LLM generates scenario to achieve objectives

Line of Effort	Event Objectives	Overall Scenario	Organization & Character Profiles	Master Scenario Event List	NPC Scenario Artifacts
1a	Developer	Developer	Developer	Developer	LLM
1b	Developer	Developer	Developer	LLM	LLM
1c	Developer	Developer	LLM	LLM	LLM
1d	Developer	LLM	LLM	LLM	LLM

* Scenario content generated prior to STARTX



Generating NPC Depth

- **Objective:** LLM generates realistic NPC interactions and decisions *

Line of Effort	NPC Action	NPC Interactions	NPC Role Player Responses	NPC Responses
2a	Developer	Developer	Developer	LLM
2b	Developer	Developer	LLM	LLM
2c	Developer	LLM	LLM	LLM
2d	LLM	LLM	LLM	LLM

* based on relationships, knowledge, and beliefs animated while exercising

Generating Infrastructure-as-Code Configurations

- **Objective:** LLM generates Terraform configurations

Line of Effort	Terraform Code Modification**	Terraform Module Creation*	Terraform Module Migration*	Terraform Error Code Corrections*
3a	Developer	Developer	Developer	LLM
3b	Developer	Developer	LLM	LLM
3c	Developer	LLM	LLM	LLM
3d	LLM	LLM	LLM	LLM

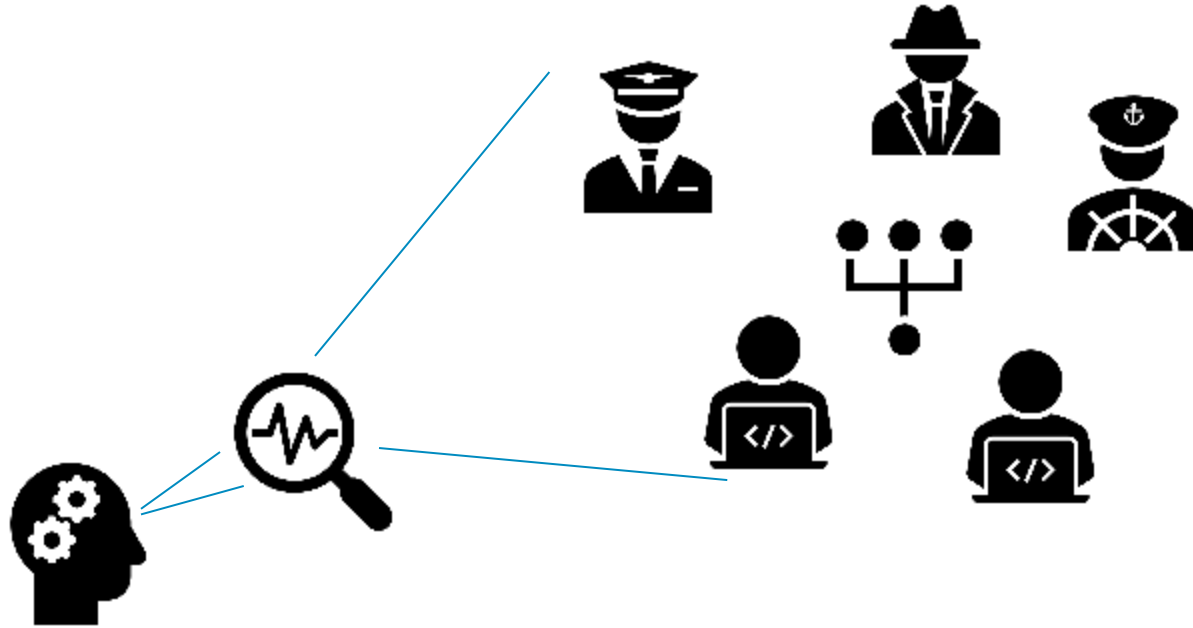
* Scenario content generated prior to STARTX

** Topology modifications generated during exercise

Other LLM Targets

- Optimize existing Kubernetes and Helm chart configurations
- Generate unit tests and code documentation
- Analyze code for vulnerabilities
- Automate/enhance monitoring of Kubernetes environment
- Automate creation of vulnerable web apps for training
- Create interactive phishing responses

Operational Readiness Testbeds



Key: Cost-Effective, Realistic Exercising Capabilities with/by Operators

Cyber Range Research and Development

Go Deeper

**Carnegie
Mellon
University**
Software
Engineering
Institute

The “Range” Problem

Lack of ability to:

Partner on platform software development \Rightarrow use open-source software

Evolve platform components \Rightarrow use modular, API-first design

Extend the platform \Rightarrow integrate available open-source applications

Customize the platform \Rightarrow select only desired components

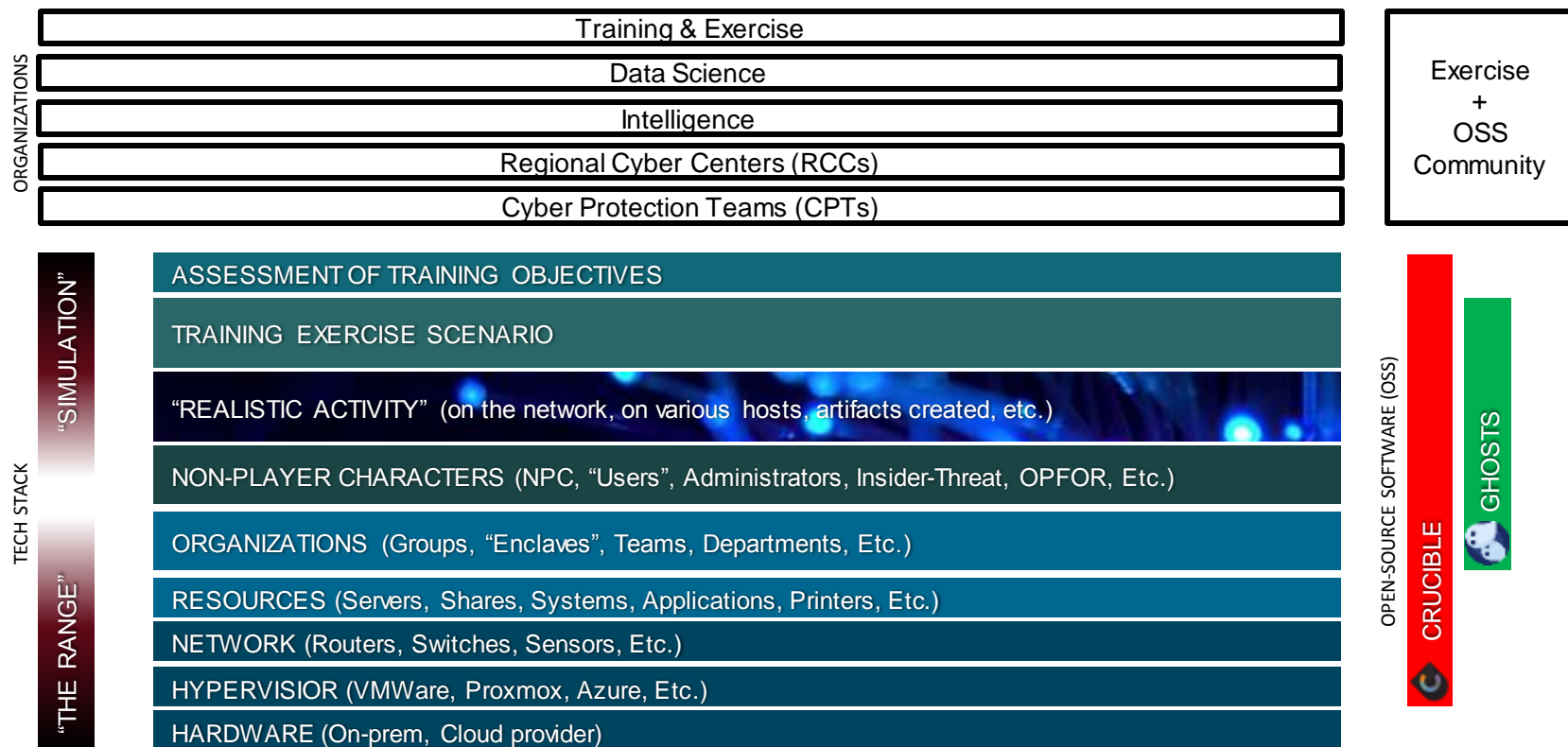
Reuse content \Rightarrow use Packer, Terraform, Ansible ‘infrastructure-as-code’ software

Interoperate \Rightarrow focus on open-standards

Deploy to different hypervisors \Rightarrow leverage Terraform resource providers

Share Information \Rightarrow adopt a federated, decentralized architecture

Cyber Range Ecosystem



Crucible



- an open-source application framework for cyber modeling and simulation
- design, deploy, and manage cyber events
- <https://cmu-sei.github.io/crucible/>

GHOSTS



- an open-source application framework for animating non-player characters
- design, deploy, and manage NPCs
- <https://cmu-sei.github.io/GHOSTS/>



VALKYRIE FRAMEWORK

- an open source suite of data science tools
- enables hunt teams to locate & identify threats hidden in network traffic
- https://github.com/cmu-sei/Valkyrie_Framework



BEACON HUNTRESS

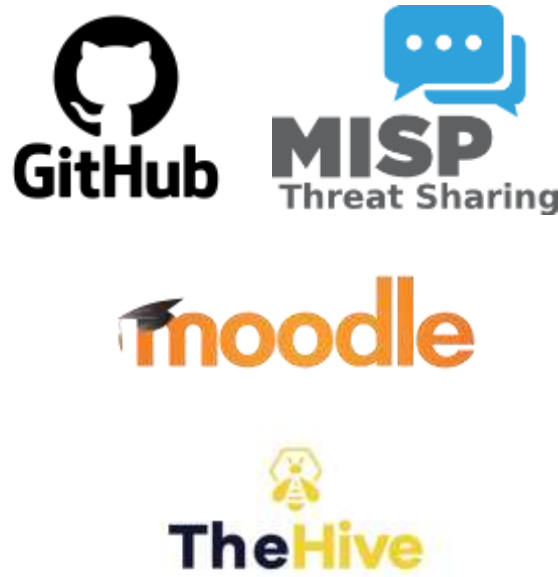
- an open-source machine-learning analytic
- identifies malicious network beacons

Cyber Range Integrations

Deployment and Configuration



Sharing and Assessment



Platform Infrastructure



Open-Source Cyber-Range Value-Proposition

DoD prefers:

- **Control:** DoD can examine, change, use Crucible & GHOSTS for any purpose
- **Partner Buy-In:** partners can share ownership and be fully invested
- **Training:** DoD can pay once for development of effective Crucible & GHOSTS training
- **Cost-Effective:** Broad-access fosters broad-adoption and use
- **Security:** DoD has ability to inspect and improve Crucible & GHOSTS code
- **Stability:** DoD avoids risk of proprietary-code 'abandonment' on long-term projects
- **Standardization:** open-standards for information sharing and capacity building
- **Community:** can produce, test, use, promote, and affect 'their' Crucible & GHOSTS
- **Interoperability:** partners can easily cooperate with each other on using Crucible & GHOSTS