CMU Support to Cyber Capacity Building

Rick Luz | Team Lead

David Tileston | Cyber Security Engineer

Operational Readiness & Evaluations
CERT Cyber Workforce Development

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

DM22-0641

Agenda

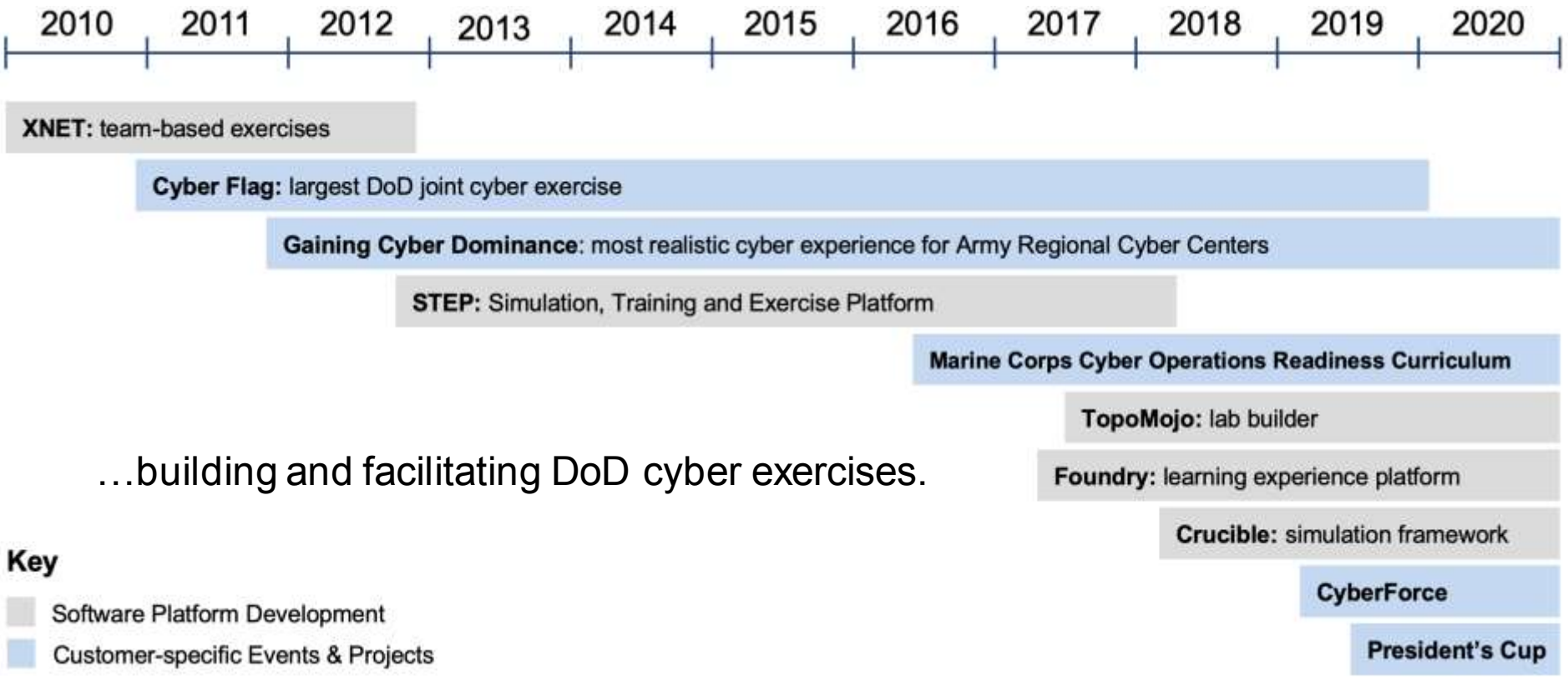
- Introduction & Background
- Support to Cyber Capacity Building
  - Cyber Endeavor
  - Crucible Simulation Framework
  - Gauntlet in the Cloud

CMU Software Engineering Institute (SEI)

- Founded in 1984 by DoD as the only R&D software engineering FFRDC
- Focus on software engineering, cybersecurity and artificial intelligence research
- ~730 total employees
- Headquarters in Pittsburgh, PA; Other offices near strategic partners in CA, MA, MD and VA

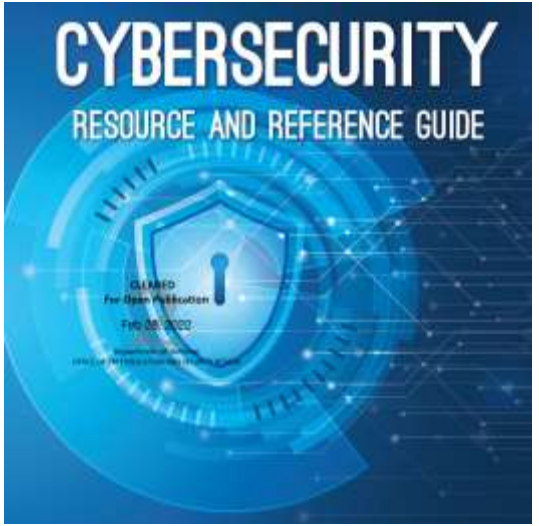
CMU Campus – Global Research University

- Global research university known for its world-class, interdisciplinary programs in computer science, machine learning/artificial intelligence, engineering, business, arts, policy, and science
- Ranked #1 for Computer Science; #1 for AI; #4 for College of Engineering
- 1,442 total Faculty and 130 Research Centers



Cyber Capacity Building

- Developing a Cybersecurity Strategy and Supporting Policies
- Building Defensible Networks and Protecting Networks from Incidents
- Critical Infrastructure Protection
- Managing Access in Systems and Data
- Building and Maintaining a Cyber Workforce
- **Build Cyber Capacity**
- **Information Sharing**
- **Interoperability**



***Influenced by standards, frameworks, and academia**

Cyber Endeavor

- Cyber Endeavor is a multi-national event where U.S. partner nations and INDOPACOM get together to build cybersecurity capacity and promote information sharing.
- Participants are invited from multiple countries to transfer knowledge, build cyber skills, and enhance cooperation through a facilitated event.
- Event leveraged a regionally deployed cloud based solution to ensure a high fidelity and reliable user experience.
- CMU used open-source software and open code technology as a basis for the platform.
- Solution leveraged CMU's Crucible Simulation Framework

Cyber Endeavor Knowledge Transfer Methodology

- Instructor/Mentor Approach
  - Facilitator led—CMU provide initial hybrid instruction through Zoom or MS Teams aligned to learning objectives
  - Hands-on, high fidelity virtual environment. Approach includes learning objectives, which provides a checks and balance for progress during hands-on/lab work (incorporating NIST frameworks into Moodle learning competencies ISO Cyber Endeavor 2022)
  - Protect the Flag HADR event
  - Future integration of President's Cup Content

An open-source cyber training platform.

Maximize **content reuse** & repeatability

- Infrastructure as code

Maximize **modularity**

- API-first

Maximize **extensibility** -- easily integrate third-party applications

- Leverage open source and existing technologies where possible

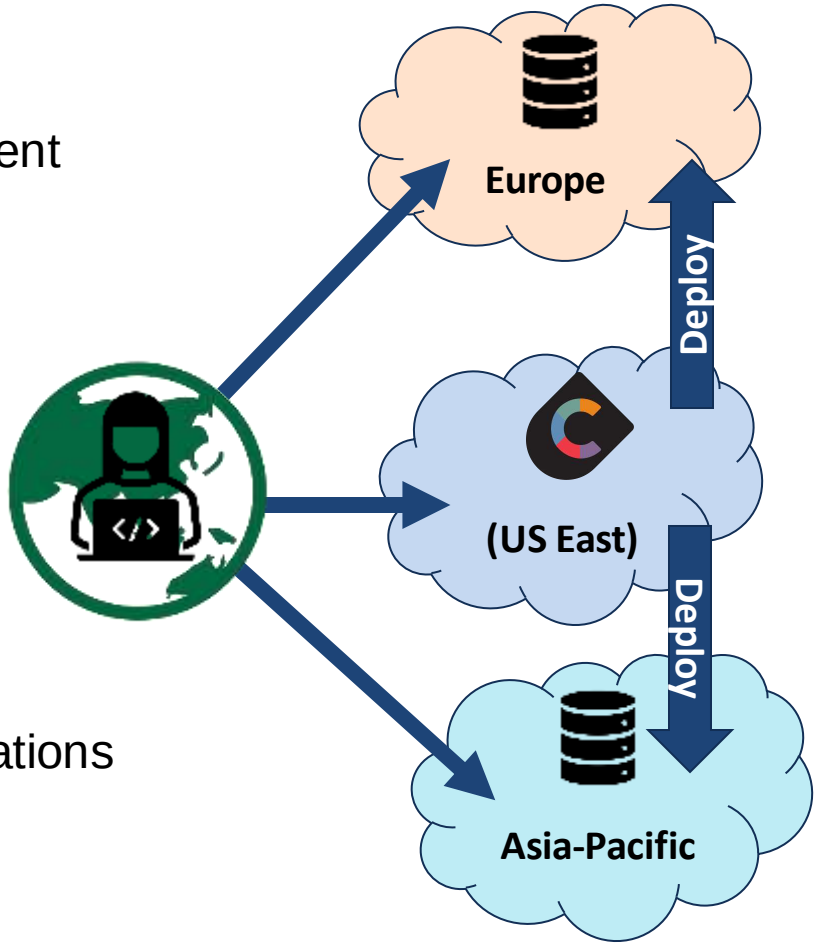
Maximize **customization** and flexibility for content developers

Maximize the use of **open-standards**

Dynamic HTML5 interface with Angular components

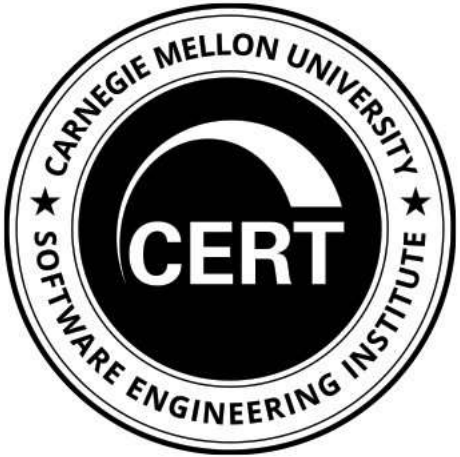
Way Ahead

- On-demand, **global access** to learning content
- **Platform-agnostic**
  - Supports variety of cloud providers
  - Deploy to local datacenters
- Reduced **costs**
- **Integration** and collaboration with partner nations



.

Questions



Crucible Core Components

Player

Caster

Steamfitter

Alloy

SEER

Player: The User-Experience App

- Primary user-facing application where teams engage in training labs or exercises
- Supports multiple teams/users per event
- Customizable interface provides access to virtual machines, documentation, and links to other apps

Caster: Topology Design & Deployment

- Topology design and deployment tool
- Utilizes open-source applications to provide infrastructure-as-code functionality
  - Terraform
  - Gitlab

Steamfitter: Scenario-Event Design & Execution

- Orchestration tool that allows exercise administrators to design a series of tasks to execute on virtual machines
- Event facilitators can monitor and control task execution or allow users to manually execute tasks
- Utilizes the open-source Stackstorm event automation engine

Alloy: The On-Demand Event Creator & Launcher

- Combines for an on-demand crucible event:
  - Player's interface
  - Caster's topology definition
  - Steamfitter's task schedule
- Users who launch an event can invite others to participate
- Events can be scored and results retained for future analysis and comparison

SEER: Team Performance Assessment

- Enables assessment and comparison of team performance of mission-essential tasks
- Maps training objectives to scenario events/injects to performance assessments
- Utilizes TheHIVE, an open-source security incident response platform

Crucible Open-Source Extensions

- CMU Developed:
  - IdentityServer ‘OpenID Connect’ authentication and identity management
  - GHOSTS NPC orchestration
  - WELLE-D Wireless network emulation
  - Topgen Internet service simulator
  - Greybox Internet simulator on a single VM
- Third Party:
  - Moodle Learning management system
  - osTicket Service-Desk system
  - Mattermost ChatOps

For more information:

https://sei.cmu.edu/go/crucible

https://cmu-sei.github.io/crucible

https://github.com/cmu-sei/crucible

or email us at:

info@sei.cmu.edu

Crucible Roadmap

- VLAN management
- User-activity statistics
- Caster “easy-mode”
- Azure-cloud hypervisor support expansion
- Terraform module expansion
- Cyber-challenge competitions
- oVirt/KVM hypervisor support
- Possible migrations:
  - Identity -> Keycloak
  - Mattermost -> RocketChat