Open-source Platforms, Tools, and Techniques for Immersive Cybersecurity Training

David Tileston

Brandon Wolfe

Modeling, Simulation and Exercises
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.

DM22-0319

Agenda

- Introduction and a brief history
- Our approach to training
- Anatomy of a cyber training event
- Training platform components
- Why open source?
- Tools for enhancement
- Use cases
- Conclusion & Questions

Carnegie Mellon University (CMU)

Pioneering discoveries that enrich the lives of people on a global scale

- Turning disruptive ideas into success through leading-edge research
- 2021 *U.S. News and World Report* rankings:
  - #1 in computer engineering, AI, cybersecurity, and software engineering
  - #2 in overall computer science
  - #3 in data analytics/science

CMU Software Engineering Institute (SEI)

Bringing innovation to the U.S. government

- A Federally Funded Research and Development Center (FFRDC) chartered in 1984 and sponsored by the DoD
- Leader in researching complex software engineering, cyber security, and artificial intelligence (AI) engineering solutions
- Critical to the U.S. government's ability to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

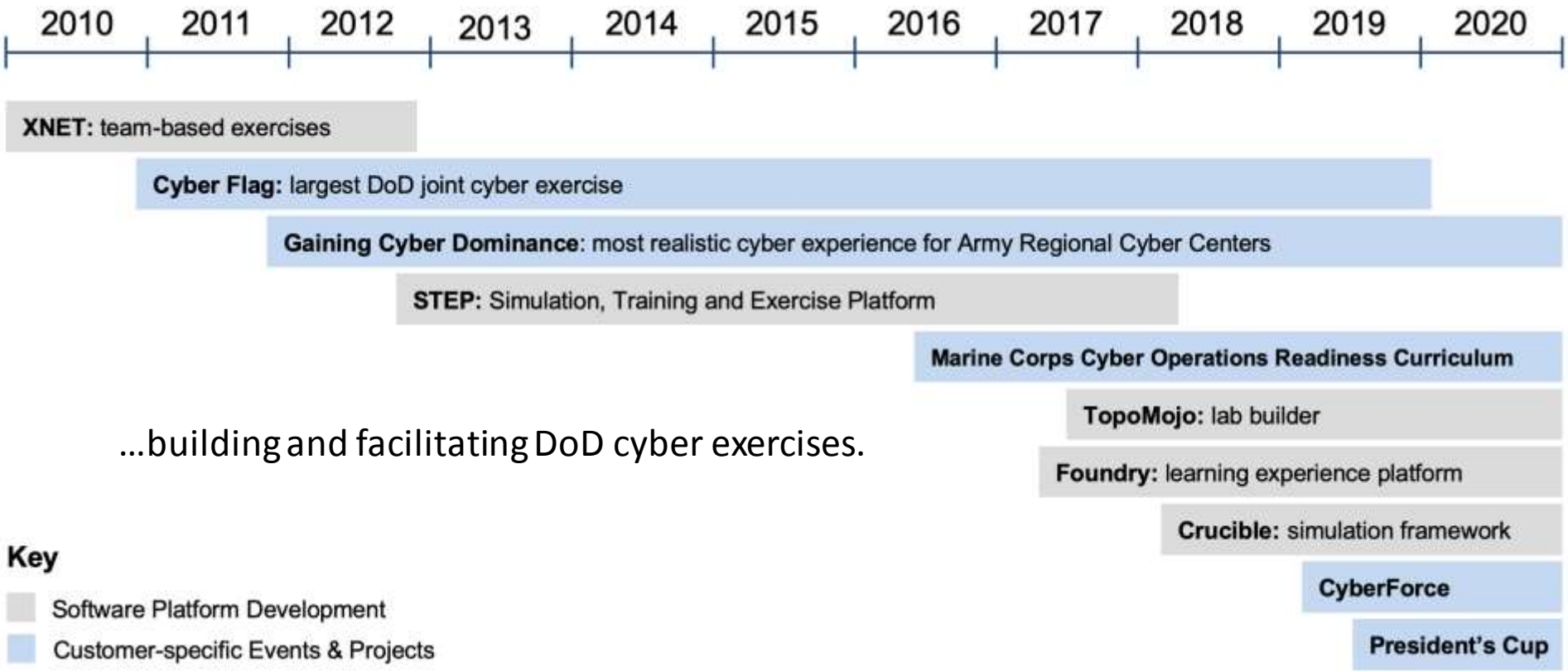
CERT Division: Birthplace of Cybersecurity

Trusted
Conducting research for the U.S. Government in a non-profit, public-private partnership

Valued
Collaborating with military, industry, and academia globally to innovate solutions

Relevant
Achieving technology and talent results for our mission partners

Our experience



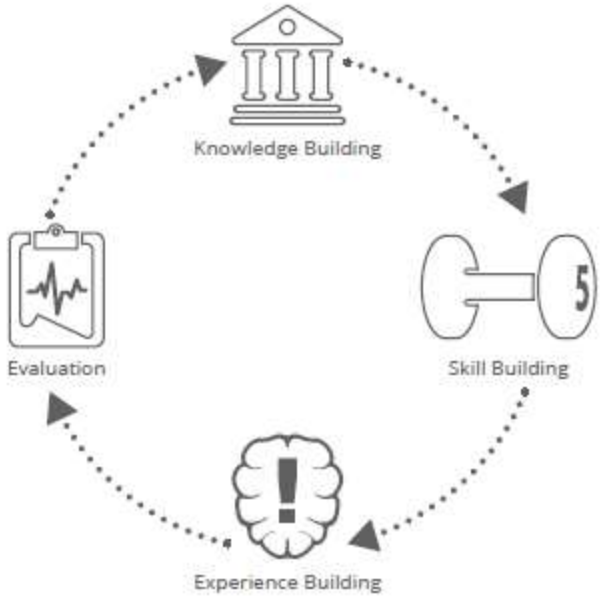
Our Approach to Cyber Workforce Development

- Map curriculum and learning content to standard public frameworks
- NICE framework -- **KSA**s
  - **K**nowledge of fundamentals
  - Technical **S**kill development
  - **A**bility to complete tasks
- Establish desired outcomes
- Measure and evaluate of performance using qualitative and quantitative metrics

Image Credit: Natasha Hanacek/NIST
https://www.nist.gov/image/16itl013niceframeworkpng

Our Approach to Cyber Workforce Development

- Content focused on individuals, teams, and organizations
- Utilize variety of content types
  - Assessment-capable video
  - Branching and adaptive text instruction
  - Interactive VMs and hands-on environments
- Measurement and tracking of accomplishments
- R&D into micro-badging and standardized credential tracking



Anatomy of a training event

1. Define desired outcomes
2. Create event scenario and supporting documentation
3. Create environment topologies and supporting infrastructure
4. Manage event participants
5. Run the event and collect measurements
6. Review event for lessons learned
7. Collect and distribute metrics and learning measurements

Training platform components

- Learning Management System (LMS)
  - Static learning materials and documentation
  - Tracks knowledge, skills, and abilities
- Environment platform for management of:
  - Users
  - Virtual machines and networks
  - Infrastructure of environment
- Training Environments
  - Single largescale network of virtual machines
  - Duplicated or on-demand small scale networks
  - No virtual machines at all

Why open-source?

- FFRDC work already licensed to DoD in perpetuity
- Recognized value in release to general public
- Existing ecosystem of open-source tools
- Need for interoperability with existing platforms
- Ability to deploy virtual machines independent of vendor environments
- Free as in beer

Crucible Simulation Framework

Crucible is an open-source application framework for cyber modeling and simulation. Its core applications provide tools to design, deploy, and manage training labs and exercises, both facilitated and on-demand.

Player

Caster

Steamfitter

Alloy

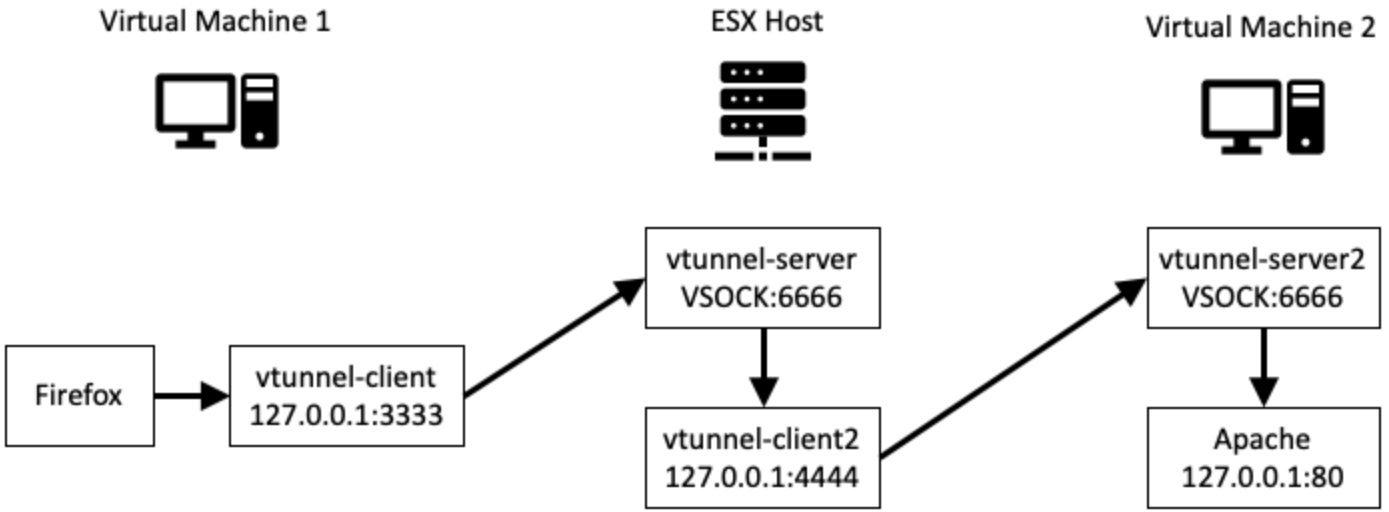
SEER

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

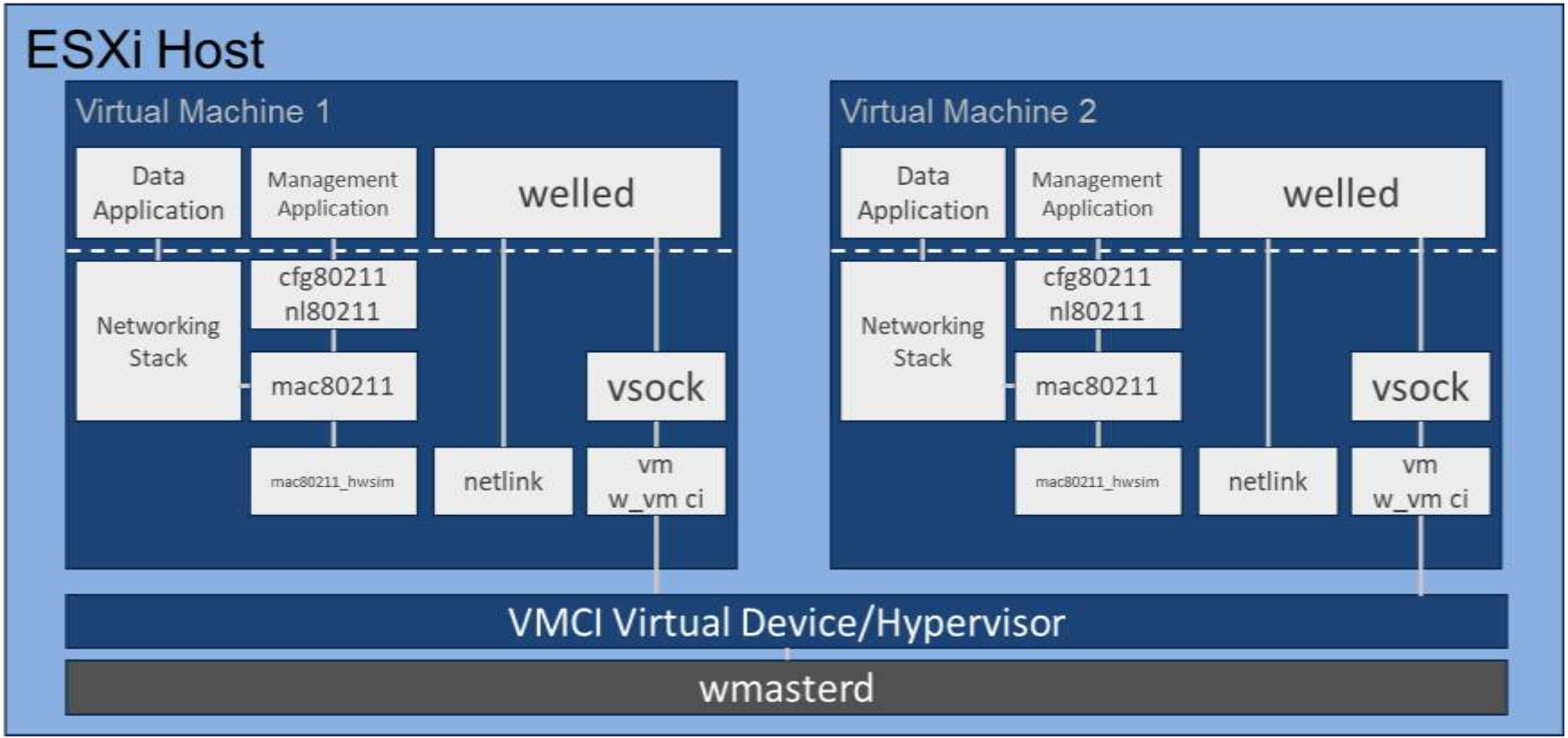
Additional Open-Source Tools

vTunnel

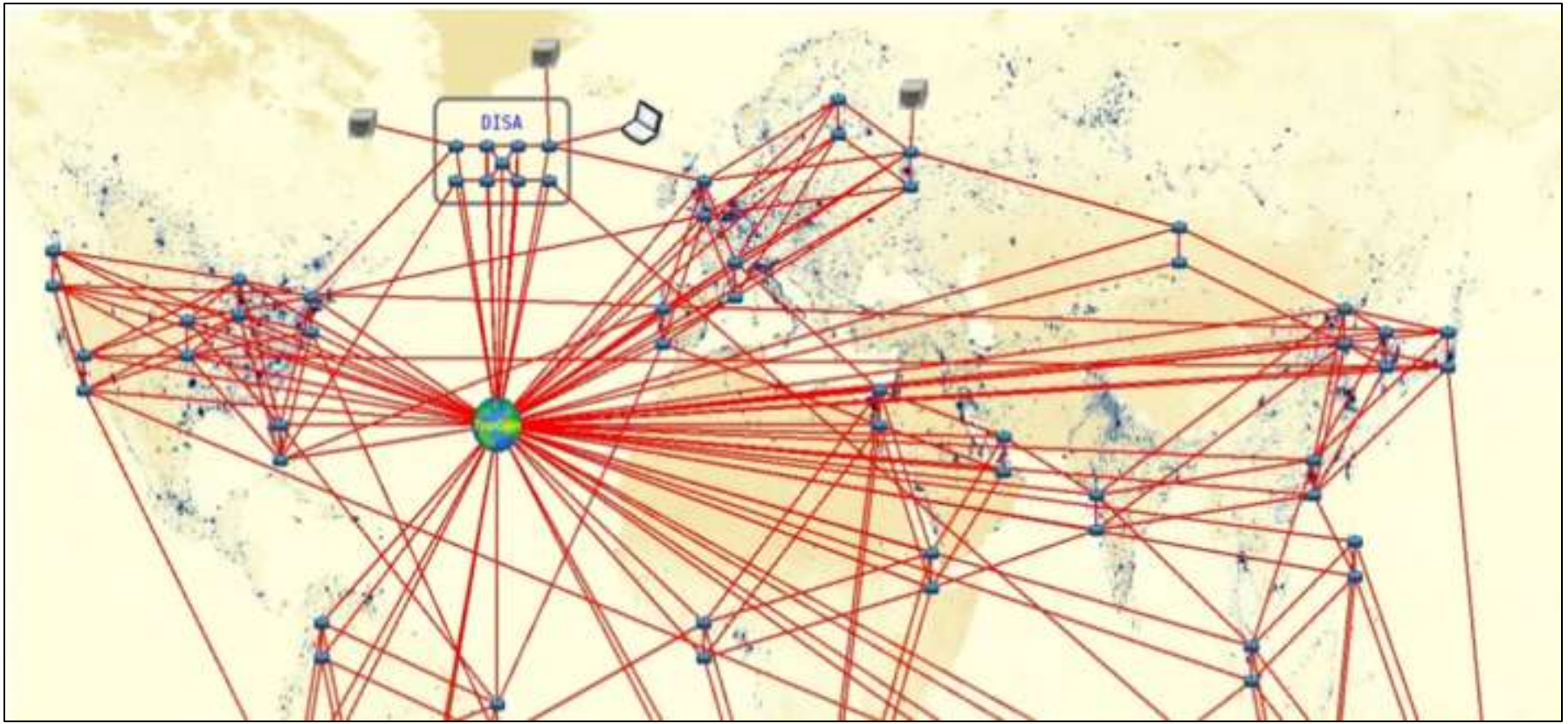


GHOSTS

WELLE-D

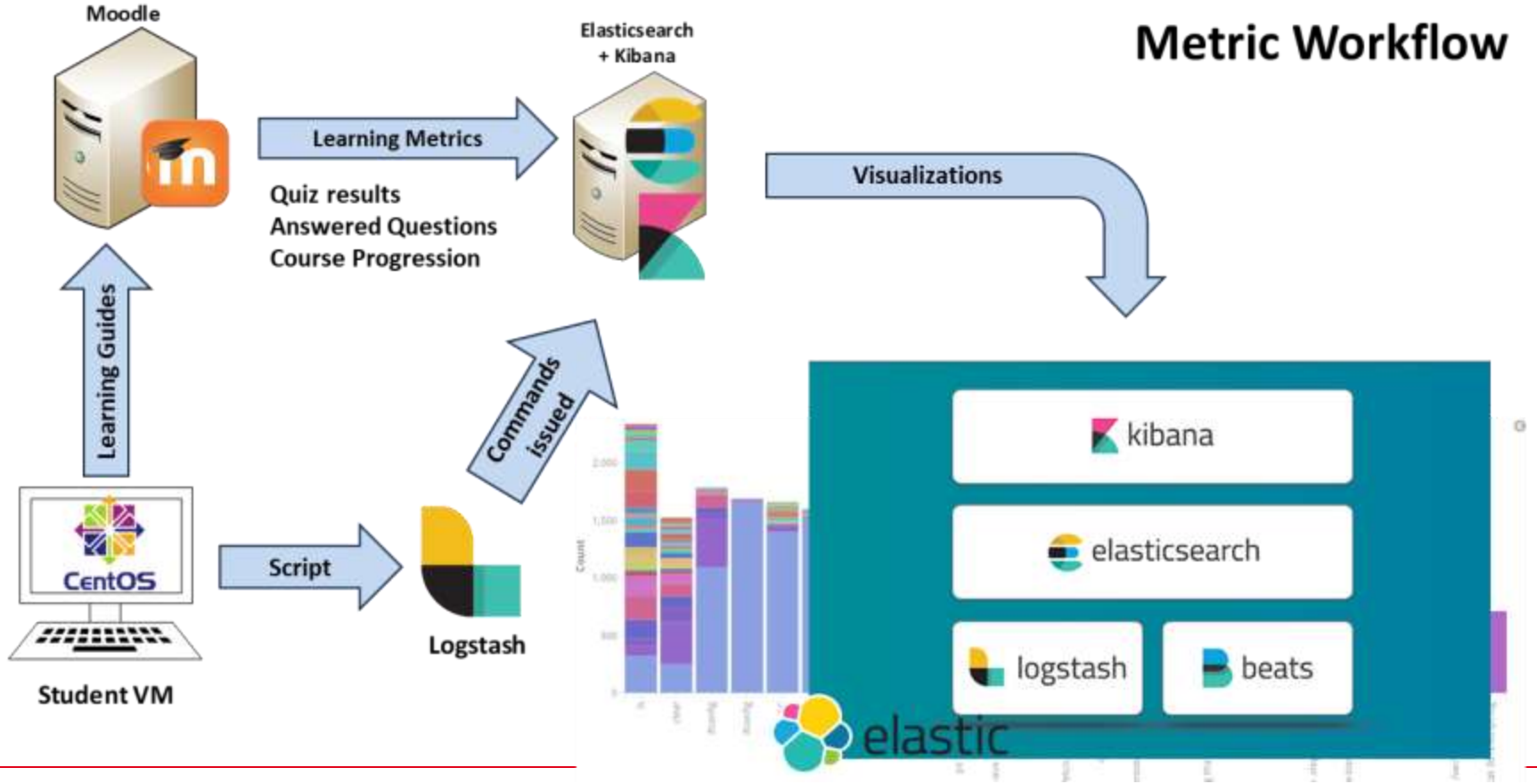


TopGen & GreyBox



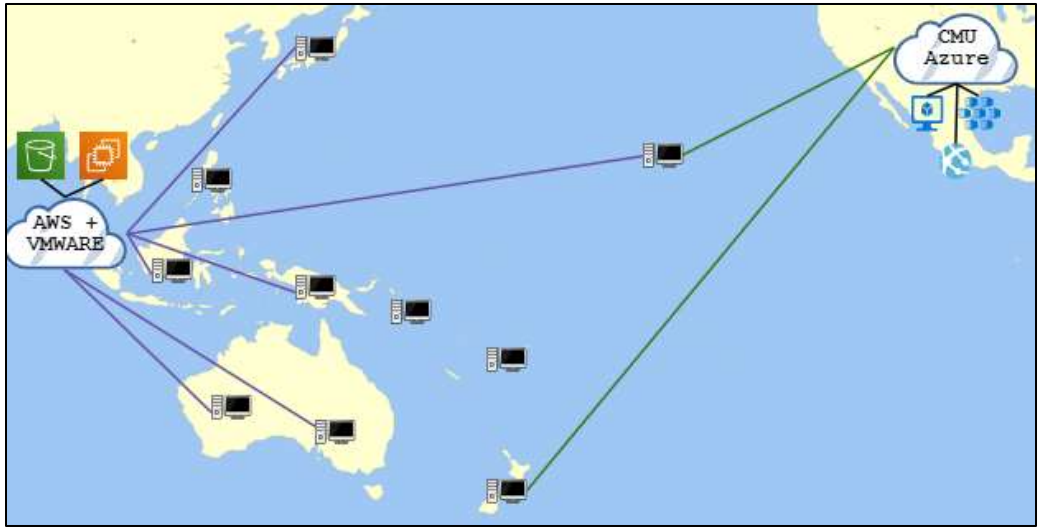
Use Cases

Use Case: Cyber Operations Readiness Curriculum



Use Case: International Exercises

- Multinational exercise with Asia-Pacific partner-nations
- Focused on building communication, partnerships, and enhancing cyber-readiness
- Use of open-source software a keystone of event
  - Allows partner-nations to utilize tools on their own
- Hybrid-cloud approach with AzureGov East and AWS Pacific



Use Case: CISA President's Cup

- Cyber competition among federal executive workforce solving challenges
- 1,000+ individual and team participants
- Platform and challenges released as open-source

https://presidentscup.cisa.gov/

Engage with Us

Download software and tools

Participate in education offerings

Attend an event

Search the digital library

Read the SEI Year in Review

Explore our research and capabilities

Collaborate with the SEI on a new project

Contact Us

Carnegie Mellon University
Software Engineering Institute

4500 Fifth Avenue
Pittsburgh, PA 15213
888-201-4479
info@sei.cmu.edu
www.sei.cmu.edu

cmu-sei.github.io
github.com/cmu-sei