Crucible

a cyber simulation framework

John W. Yarger
Technical Manager, Mod/Sim and Exercises Initiative
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.

DM20-0809

Introductions

Product Champions

John Yarger

Peter Barrett

Dev Team

Ryan Lehman

Chad Hershberger

Andrew Schlackman

Tim Spencer

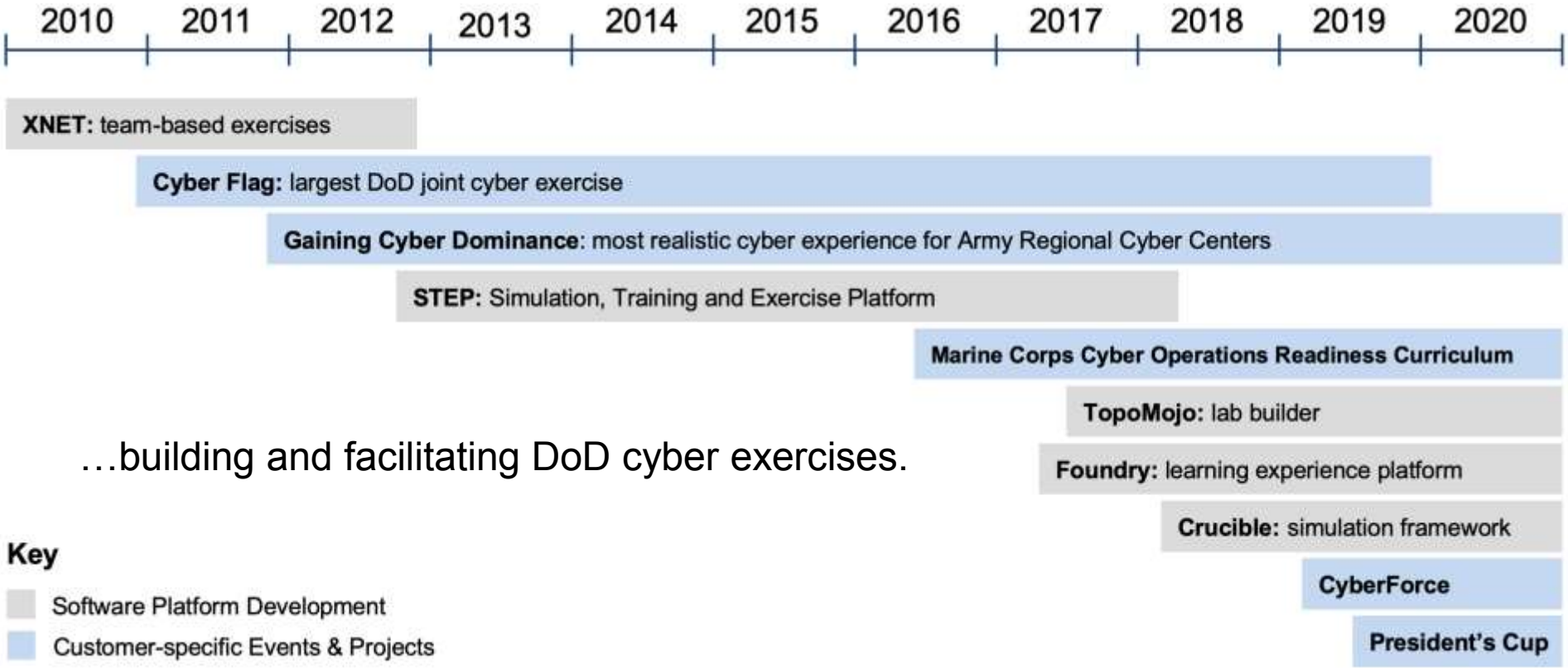
Eric Bram

Nic O’Connor

Agenda

- Motivations for building Crucible
- Crucible design goals
- Crucible framework components

Motivations:
Exploit Our Experience



…building and facilitating DoD cyber exercises.

Motivations:

Eliminate Capability Gaps

Content reuse

Build-automation

Expand Collaboration

Community of interest

- government
- academia
- industry

Open source

Applied Research

- AI/ML research
  - algorithm development
  - topology-morphing
  - human-machine teaming
- Cyber readiness:
  - mission rehearsals
  - cyber-kinetic operations
  - wargaming

…and more

Design Goals

Maximize content reuse & repeatability

- Infrastructure as code

Maximize modularity

- API-first

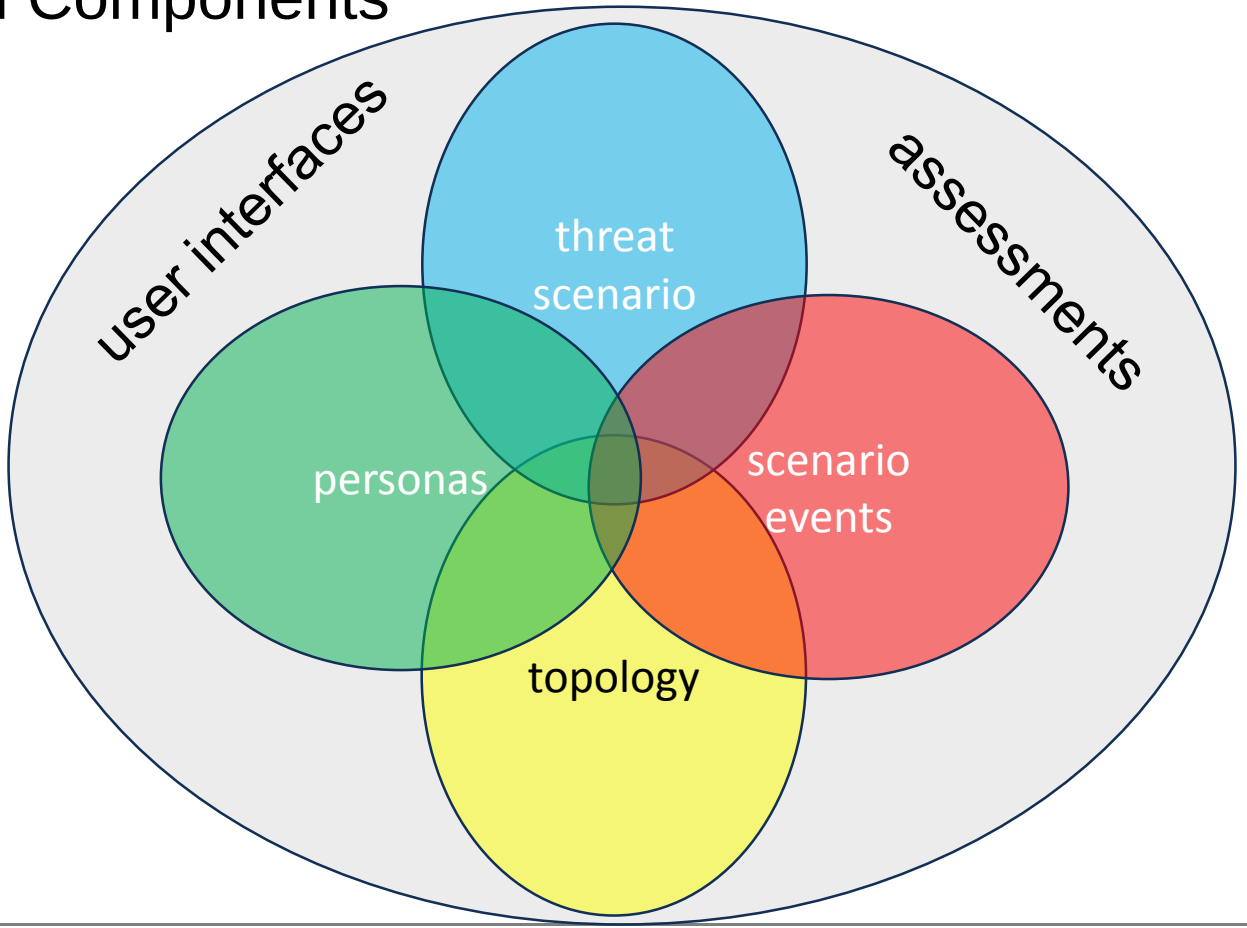
Maximize extensibility -- easily integrate third-party applications

- Leverage open source and existing technologies where possible

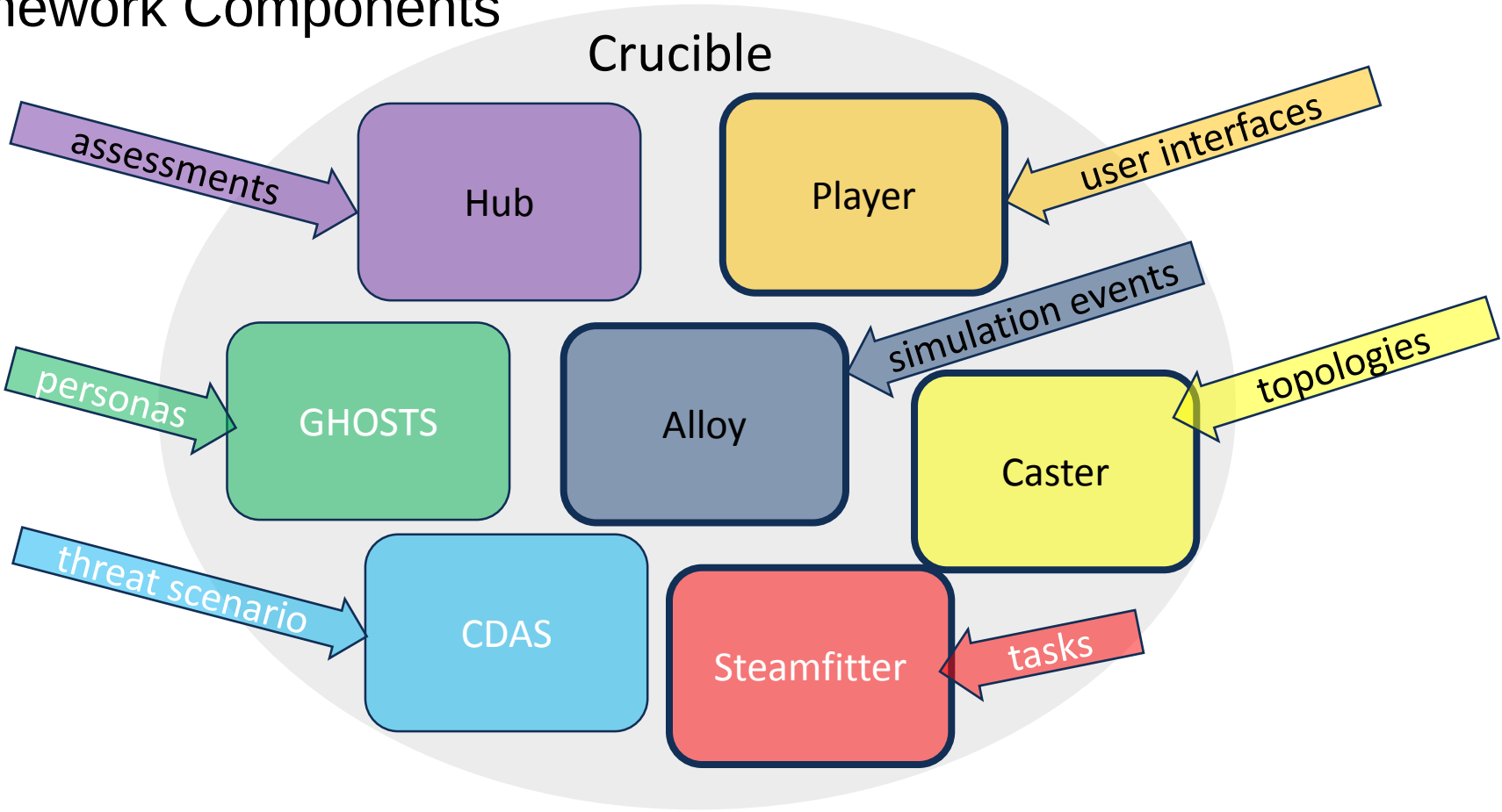
Maximize customization and flexibility for content developers

Browser-based HTML5 with Angular components

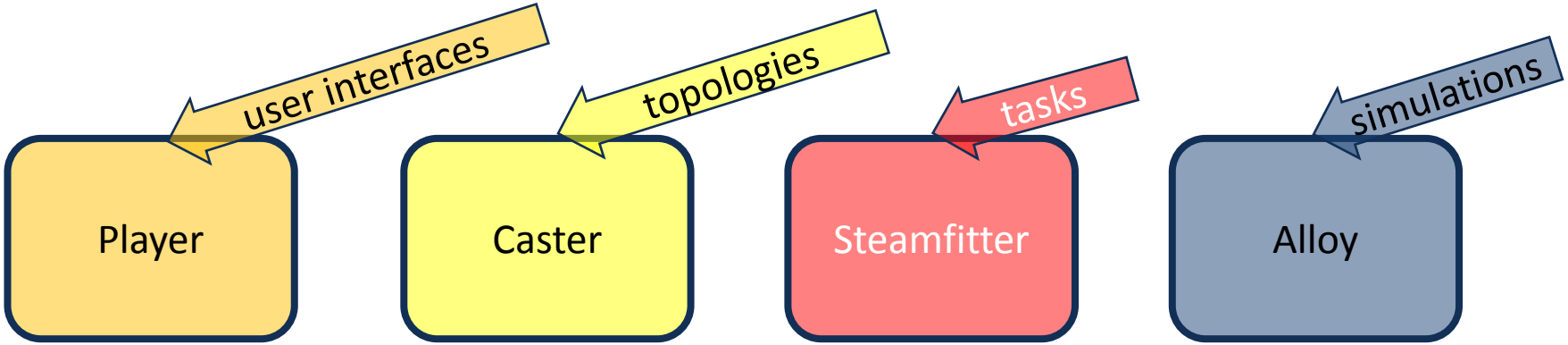
Simulation Components



Framework Components



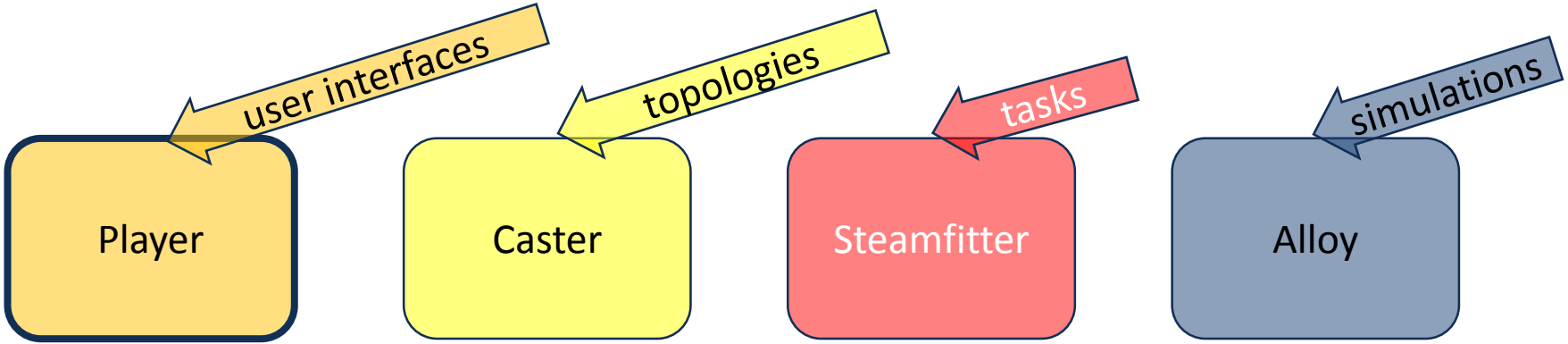
Core Crucible Applications



Crucible is a modular cyber simulation framework for creating, deploying, and managing virtual-environments and scenario-events to support training, education, and exercises.

Crucible README.md on Github

Core Crucible App: Player

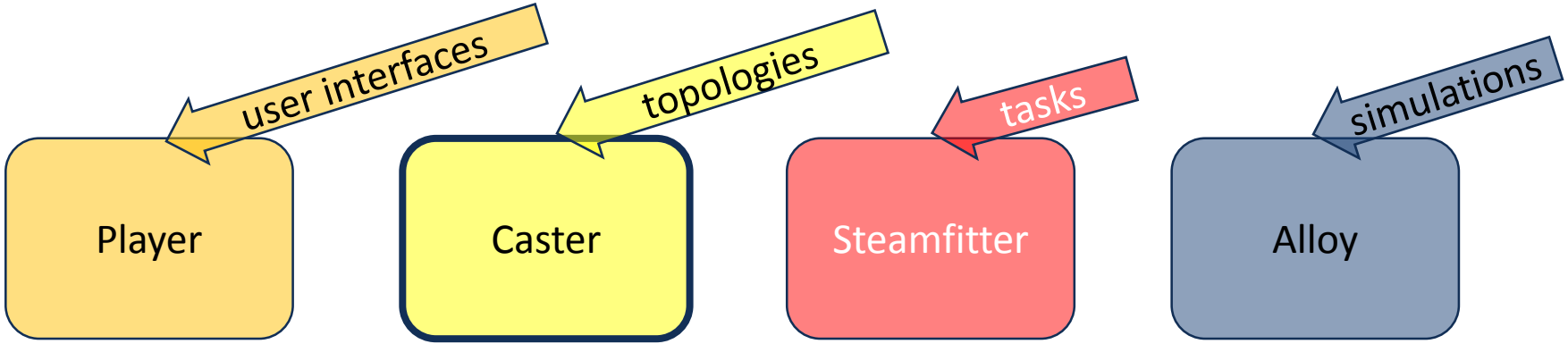


Player is the centralized interface where participants, teams, and administrators go to engage in a cyber simulation event.

- Exercise developers can configure teams, applications, virtual environments, and third-party applications.

Player UI README Player API README

Core Crucible App: Caster

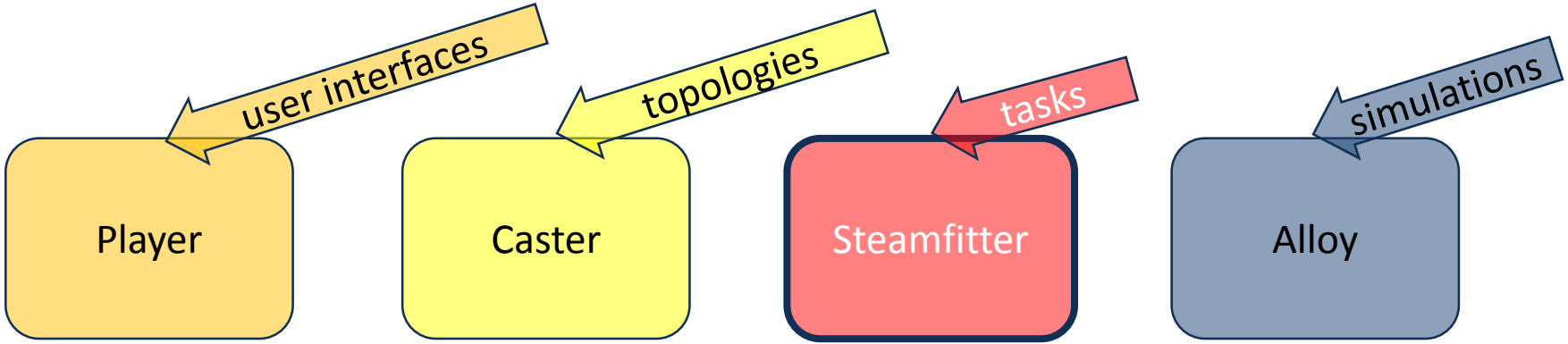


Caster enables exercise developers to the design and deploy cyber topologies – leveraging open-source applications:

- Terraform – an "Infrastructure as Code" tool.
- GitLab – a DevOps code repository.

Caster UI README Caster API README

Core Crucible App: Steamfitter

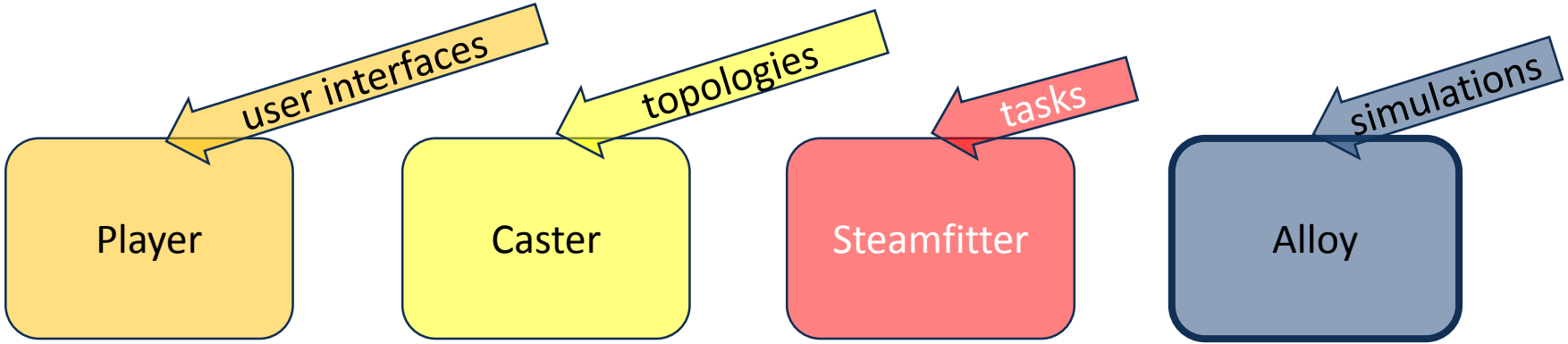


Steamfitter: enables content developer to create a series of tasks to run on virtual machines in an exercise. During an event, exercise administrators can monitor and control task-execution.

Steamfitter UI README

Steamfitter API README

Core Crucible App: Alloy

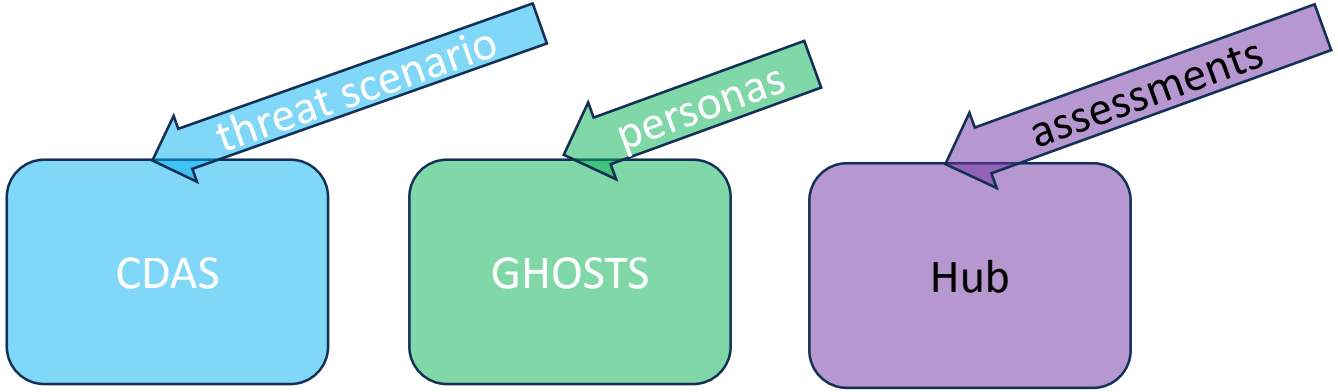


Alloy units a ‘team-structure/user-interface’, a ‘cyber topology’, and a ‘scenario template’ to create a complete Crucible simulation event.

Alloy UI README

Alloy API README

Crucible Extensions

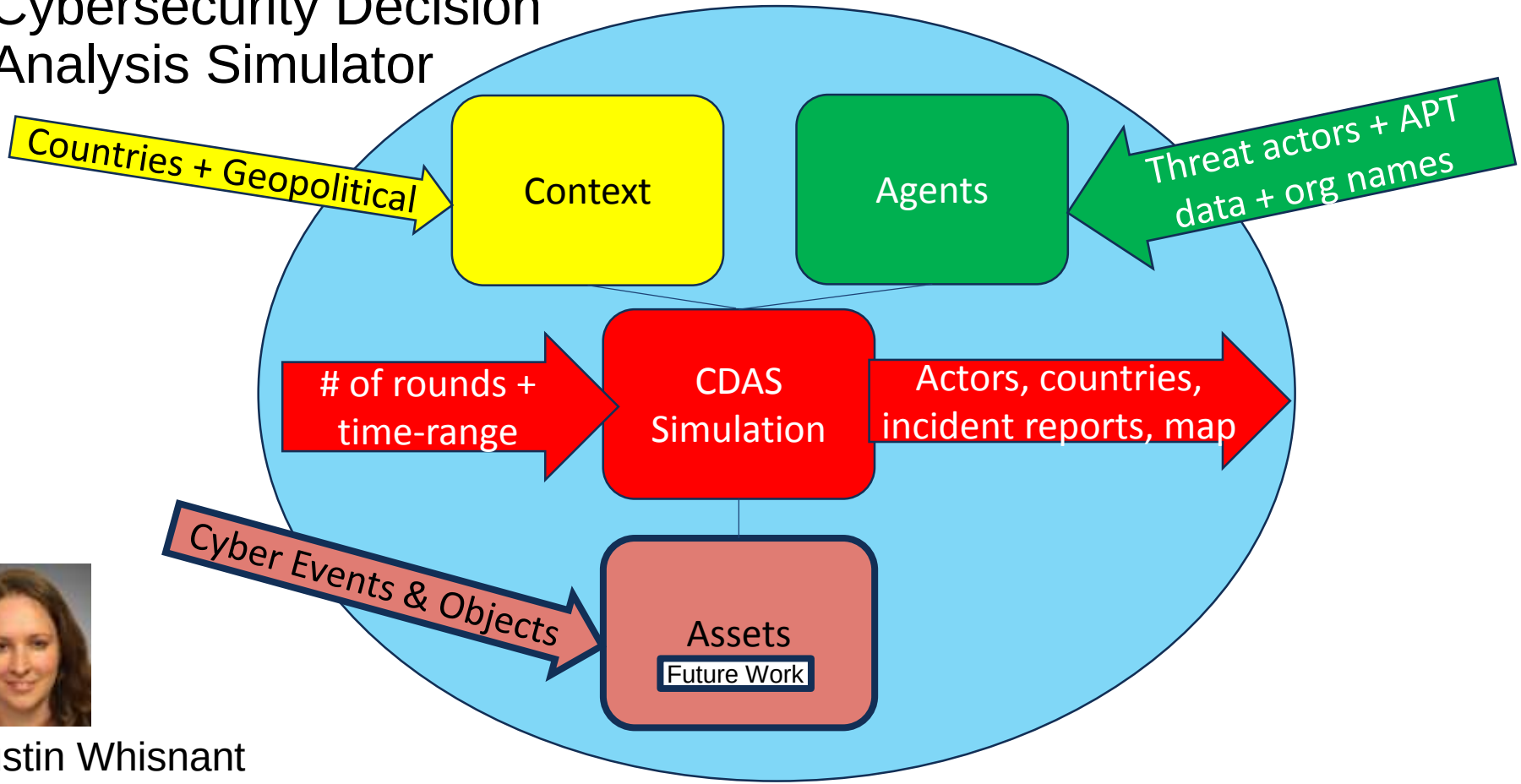


Cybersecurity Decision Analysis Simulator

GHOSTS NPC Orchestration Framework

Hub – training objectives, injects, team quizzes and embedded observer assessments

Cybersecurity Decision Analysis Simulator



Austin Whisnant

GHOSTS NPCs

Dustin Updyke

Tom Podnar

Tyler Brooks

chat & messaging

master-controller

decision-making

Timelines & configs

IP diversity & containers

User-details

HOWL

NECROMANCER & ENCHANTER

PROTOPACK

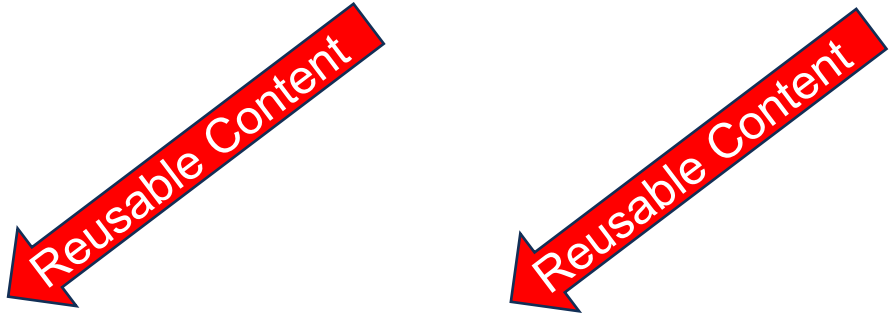
CORE Client/C2

SPECTRE

CYCLONE & STAYPUFT

ANIMATOR

Automation of a Scenario Simulation



Source Material

Seed Images
Infrastructure Code
Scripts
Injects
Data Repositories
Cyber Threat Data
Custom Seed Data

Template

Terraform Directory
Scenario Template
Player View Template
Event Template
Desired Configurations
Design Specifications
Reusable Modules

Automation Engine

Caster
Steamfitter
Player
Alloy
GHOSTS
CDAS

Simulation Event

Terraform Workspace
Scenario
View
Event
Active NPCs
Threat Scenario

Automation of Scenario Simulation

Scenario Component	Source Material	Template/Config	Automation Engine	Event
Topology	Gitlab: Terraform Modules	Directory	Caster/ Terraform	Workspace
Tasks	Scripts, Injects, Events	Scenario Template	Steamfitter/ Stackstorm	Scenario
Threat Scenario	CIA World Factbook, MITRE ATT&CK, and custom seed files	CDAS config.json: • Agents (names, APT, orgs names) • Context (country, geopolitical) • *Assets (events, objects) - TBD*	CDAS	Threat scenario simulation artifacts (intrusion sets, countries, incident reports)
Personas	Timelines, Websites, User-details	GHOSTS Config	GHOSTS	NPCs
Assessments	METLs, Wiki, Scenario-Events, Quiz Questions	Hub Config	Hub	Augmented Assessment Dashboard
Interface	Identity, Apps, Docs	View Template	Player	View

Cyber Threat Intelligence (CTI) Repository:
- Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) catalog
- Common Attack Pattern Enumeration and Classification (CAPEC) catalog
expressed in Structured Threat Information Expression (STIX) 2.0 Javascript Object Notation (JSON) file format

Cyber Data Exchange Model (CyDEM): represent cyber events (effects, action) and objects (network, link, device, app, data)

Questions?