# Sharpening Skills with Immersive Threat Hunting Experience-Building

**Modeling, Simulation, & Exercise Initiative**
CMU / SEI / CERT / CWD
17 November 2022

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.


DM22-1106

# How We Could Fit In

# Who We Are

- Cybersecurity Engineers
  - Infrastructure
  - Cyber Operations
  - Software / DevOps
  - Data Science

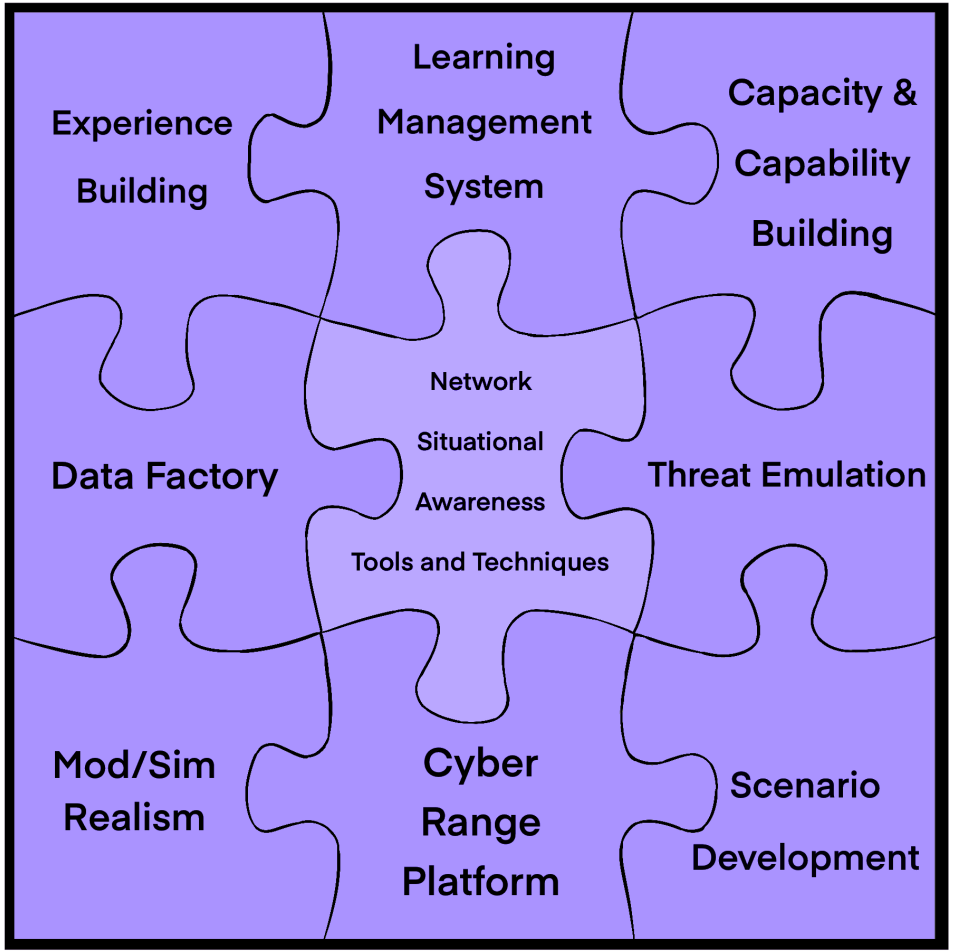
# What We Create

- Cyber ranges
- Virtual environments
- Relevant scenarios
- Typical network activity
- Emulated threat actors
- Learning experiences
- Testing environments
- Datasets

# What We Can Enable

1. Practicing on your available data sources
2. Challenging your threat hunting teams
3. Testing emerging technology
   - Edge Netflow
   - Zero Trust
   - Endpoint Detection and Response
   - Cloud
   - Artificial Intelligence / Machine Learning

# Where We Fit In…



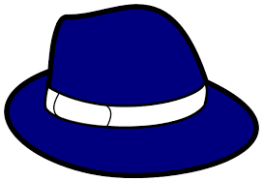
# Annual DoD Cyber Exercise Series 2012 - 2022

# DoD Cyber Exercise Program

- Fully customizable, highly realistic
- Nearly continuously funded since 2012
- Hundreds of exercises with thousands of participants over tens of thousands of exercise hours

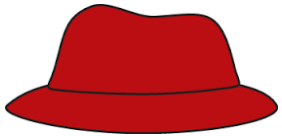
***= Deep cyber war exercise knowledge***

Cyber Range R&D, Tech Support



Role Play: Cyber Security Service Provider, Intel, Mission Owner, etc.

Scenario Design, Master Scenario Event List, Assessments



Role Play: Adversaries, Exploits

# 2022 Exercises

**Cyber Security Service Providers**
- 4-hour training exercises
- 8-hour certification exercises

**Cyber Protection Teams**
- 1-4 week training exercises
- 1-4 week APT emulation exercises

***42 exercises since February***

# Exercise Development Process

| Planning | Prep | Execution | Reporting |
|---|---|---|---|

Outputs:

- Exercise Charter
- Exercise Roster

Outputs:

- Cyber Cards
- Exercise Playbook
- Scenario Event List
- Participant Guide
- Network Validation
- Storyline Artifacts

Outputs:

- In-Game Artifacts
- Participation Report
- Exercise Assessment
- Dynamic MSEL

Outputs:

- Surveys
- After Action Reports
  - Team
  - CMU

# Building the Attack Space

# Range Topology Goals

- **Realism**
  - Align with commercial tools where possible

- **“Sufficient Complexity”:**
  - Hundreds of Windows 10 users / 13 subnet areas
  - Microsoft Active Directory & File services
  - Enclave hosted applications (portals, business process management, etc.) / DMZ’s

  - **Traffic generation**
    - Web browsing, file downloads, file sharing
    - User activity / logins/logouts
    - Endpoint protection and logging traffic

  - **Shared Internet space**
    - Point in time copies of the Internet and DNS zones
    - Geographically diverse adversary IP address space

- **Commercial software/tools**
  - ACAS / Nessus
  - Arcsight
  - Cisco ASA firewalls
  - Cisco Sourcefire / Firepower IDS
  - Virtual Cisco routers
  - Dell Quest Active Directory Change Auditor
  - F5 Proxy - TLS inspect
  - McAfee ePolicy Orchestrator
  - McAfee Network Security Monitoring (NSM)
  - Microsoft - Windows 10 / server 2016/2019
  - Splunk
  - Tychon
- **Open-Source software/tools**
  - Security Onion
  - Arkime (Moloch)
  - Elastic (ELK)

# Range Scenario Goals

- **Realism**
  - Align with **real world scenarios and intel**
  - **Library of cyber attacks / injects**
    - Seventy documented / ready to go (easy replay)
  - **APT emulation** timelines for attribution exercises
- **Full Exercise Team Participation**
  - Focus is not just technical
  - Battle captain leadership / fast pace
  - Refine team roles / workflow
  - **Increasing adaptability**
- **Cyber Data Science**
  - Continuous data source of realistic data embedded with malicious adversary activity

# CMU team responsibilities

- **Range infrastructure**
  - design / implementation / maintenance / upgrades
- **Cyber scenario development**
  - Research / develop / implement complex cyber attacks
- **Exercise control**
  - Scheduling / white cell moderation
  - Role play
    - **Higher headquarters**
      - Intel & task orders
    - **Red team**
      - Launch / control all attacks





**Remove all barriers so teams can focus on their mission**

- **Dedicated and persistent cyber ranges**
  - Every organization/team has their own range

- **Dedicated - availability**
  - 24x7 - during exercise season
  - Team scheduling flexibility

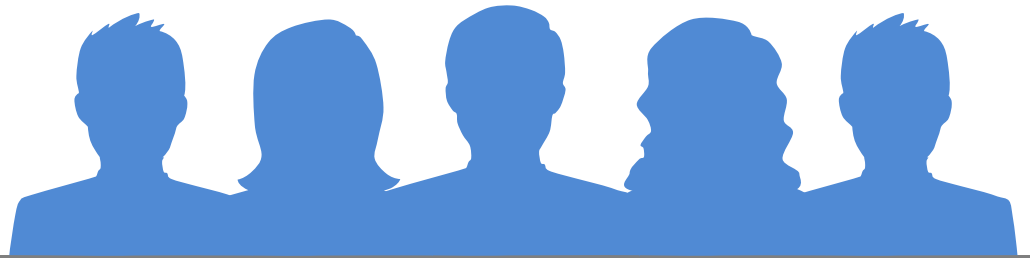
- **Persistence - range technical configurations**
  - **Baseline configs**
    - Active Directory users/groups
    - Microsoft Windows group policy objects (GPO)
    - Microsoft Windows and network event log aggregation
    - Network ACL's / firewall rules

**More team participant time for sophisticated tuning and hunting**

# An exercise contains interactions between:

- **Player**
  An active human participant

- **Non-player character (NPC)**
  Any character not controlled by a player within the exercise



# GHOSTS orchestrates realistic NPCs that:

- Are behaviorally accurate
  - (from harmless administrators to hostile nation-state attackers)
- Represent an infinite array of possible interactions
- Are fully-autonomous
- Match training realism with high training value
- Prepare cyber warfare teams for success in real-world situations

# Sydney Zackariah Deutschmann

Home | Education & Career | Insider Threat | Military Service | Relationships

**First name**
Sydney

**Last name**
Deutschmann

**Biological Sex**
Male

**Height / Weight**
74"/ 197 lbs.

**Blood Type**
O+

**Location**
07/18/1982

**Phone**
(390) 001-3019

**Mobile**
(061) 901-5625

**Primary Email**
sydney.zackariah.deutschmann.mil@mail.mil

**Password**
^w6]5<U%

## Addresses

### Home

350 Shirinlou Bridge Coffeeville, Mississippi 38922

## Default Workstation

**flag-18.local (192.168.244.52)**

sydney.zackariah.deutschmann / teasley.mil

## PGP Key

**sydney.zackariah.deutschmann.mil@mail.mil (*]n_Q96b)**

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: BCPG C# v1.8.6.0

lQHqBF8HVs8BBACJVmHBVXGAuSPZDBGgQX/90SgK57fSP2vx41j7NvPYrOcalFjq
9PU0gL6cYNx3E+8EXHpBYfN3Dyr7RSKpLsyh3Alb+wn/znneuCQ3tWJINMmgYYQH
```

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG C# v1.8.6.0

mIsEXwdWzwEEAIlWYcFVcYC5l9kMEaBBf/3RKArnt9l/a/HjWPs289is5xqUWOr0
9TSAvpxg3HcT7wRcekFh83cPKvtFlqkuzKHcAhv7Cf/Oed64JDe1Ykg0yaBhhAff
```

## CAC

CAC not on file

Build Details

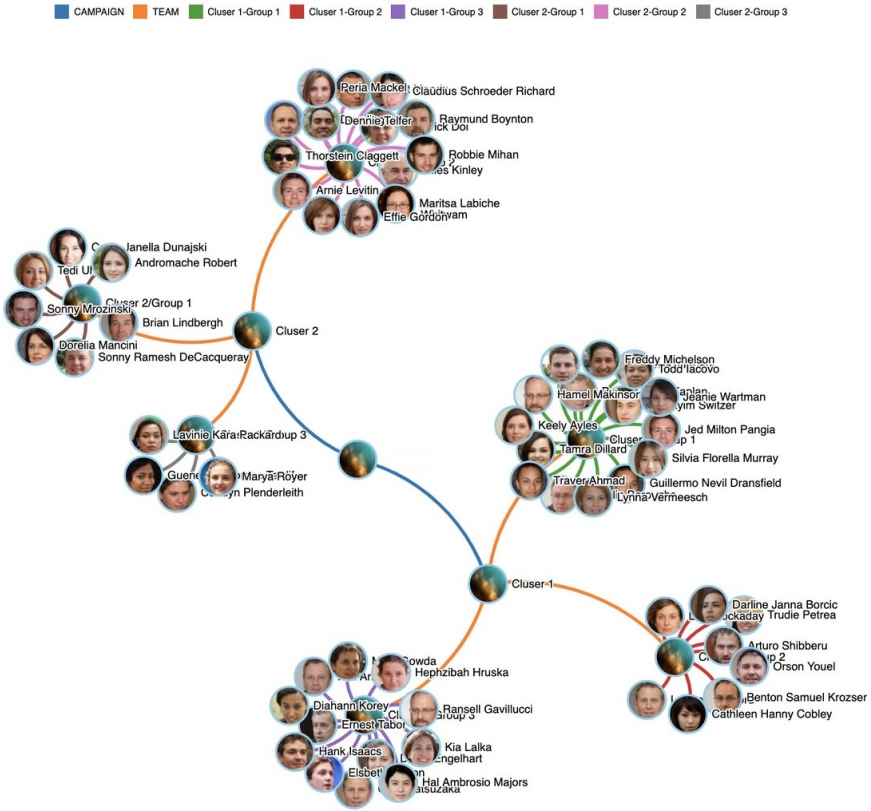
Created: 07/09/2020
Campaign: GCD 2021
Enclave: RCC-K
Team: INTEL

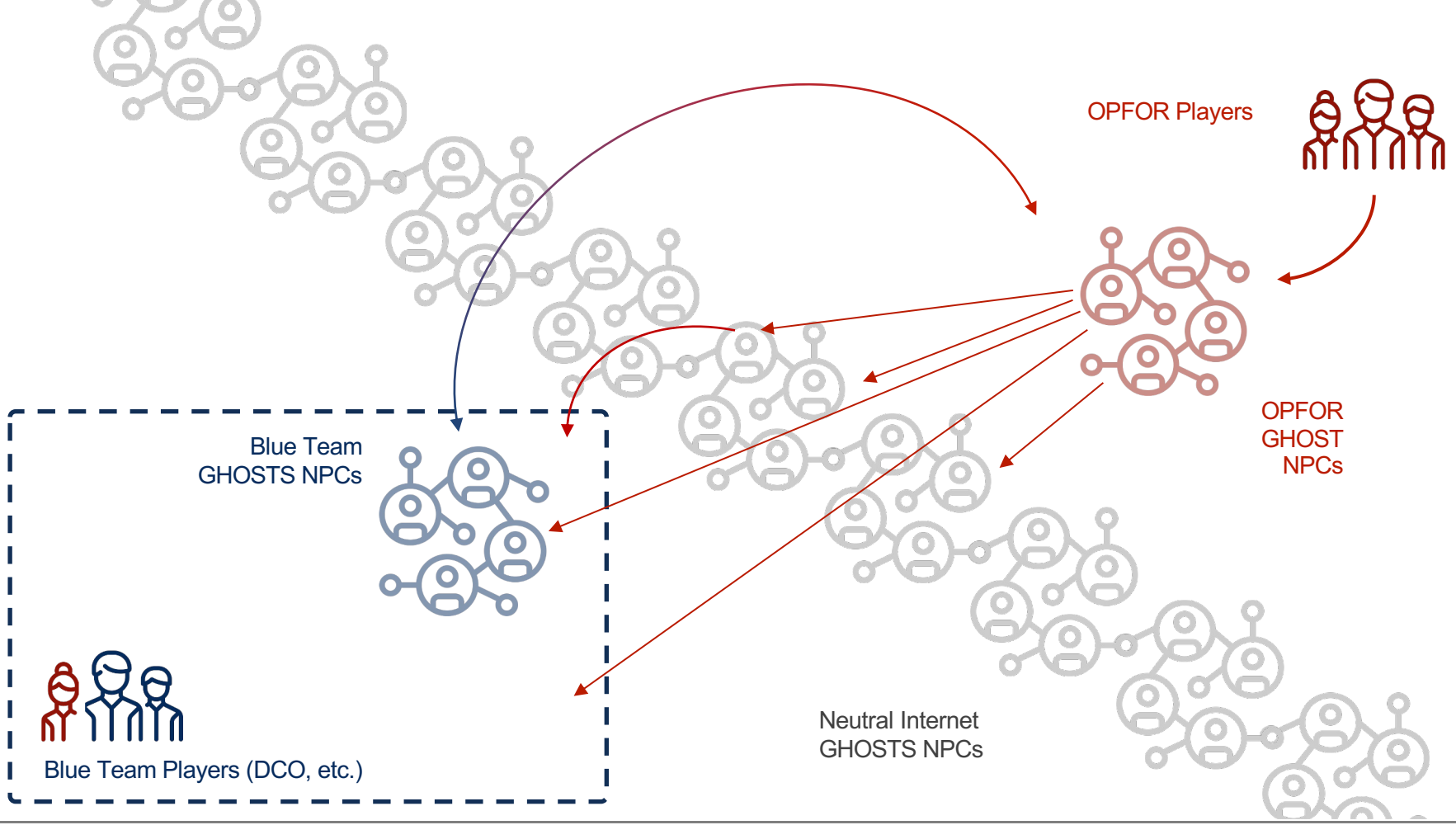
| Accounts | |
|---|---|
| sydneyzacka2481 | @Signal |
| Psychohobo | @Tumblr |
| sydneyzackariahdeutschmann | @gmail |
| sydn4385 | @Youtube |
| sydneyzackariahdeutschmann | @Facebook |
| sydneyzackariahdeutschmann8609 | @LinkedIn |
| sydneyzackariahdeutsc9418 | @Twitter |
| WillaryClinton | @http://gilstorf.us |
| try_to_cook_stuff | @http://coffey.uk |
| sydneyzackariahdeutschmann | @http://boehlke.biz |
| sydneyzackar6146 | @http://ashworth.com |
| sydneyzackariahdeutschm9733 | @http://feith.co.uk |

# Animator Build Relationships

A view of related NPCs generated from GHOSTS ANIMATOR ON Monday, 09 November 2020.

Build: 9c427e49-1eb0-46fa-9a9f-0805dce4456c





# Our Ecosystem

**CYBER-OPERATOR MONEYBALL**
"WHO IS GOOD AT WHAT" ML
2023

**Exercise Chat**
Admin/EO/Team comms
2023

**Range Events**
GHOSTS

**LRS**
Learning Locker

**HIVE**
OSS Security Incident Response Platform

**Inject Catalog** 😈
"A library of very bad things"

**CORTEX**
Observable Analysis & Active Response Engine

**Exercise Admin**
Range Notes

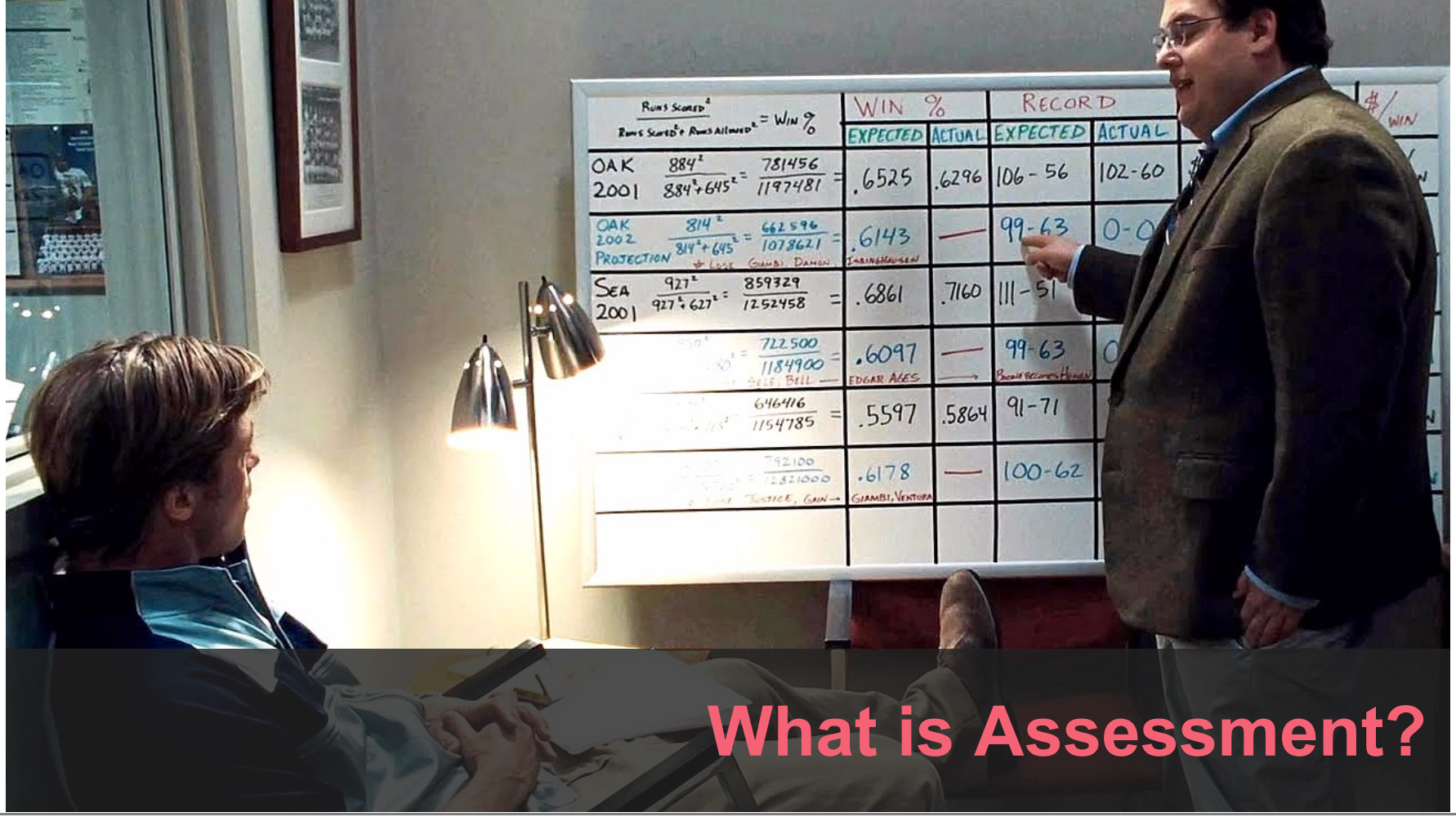
**External Assessor**
Assessment Score & Notes

PARTICIPANT SELF-REPORTING

MISP Threat Sharing

**MISP**
OSS Threat Intelligence Platform

**SEER**
Assessment Platform

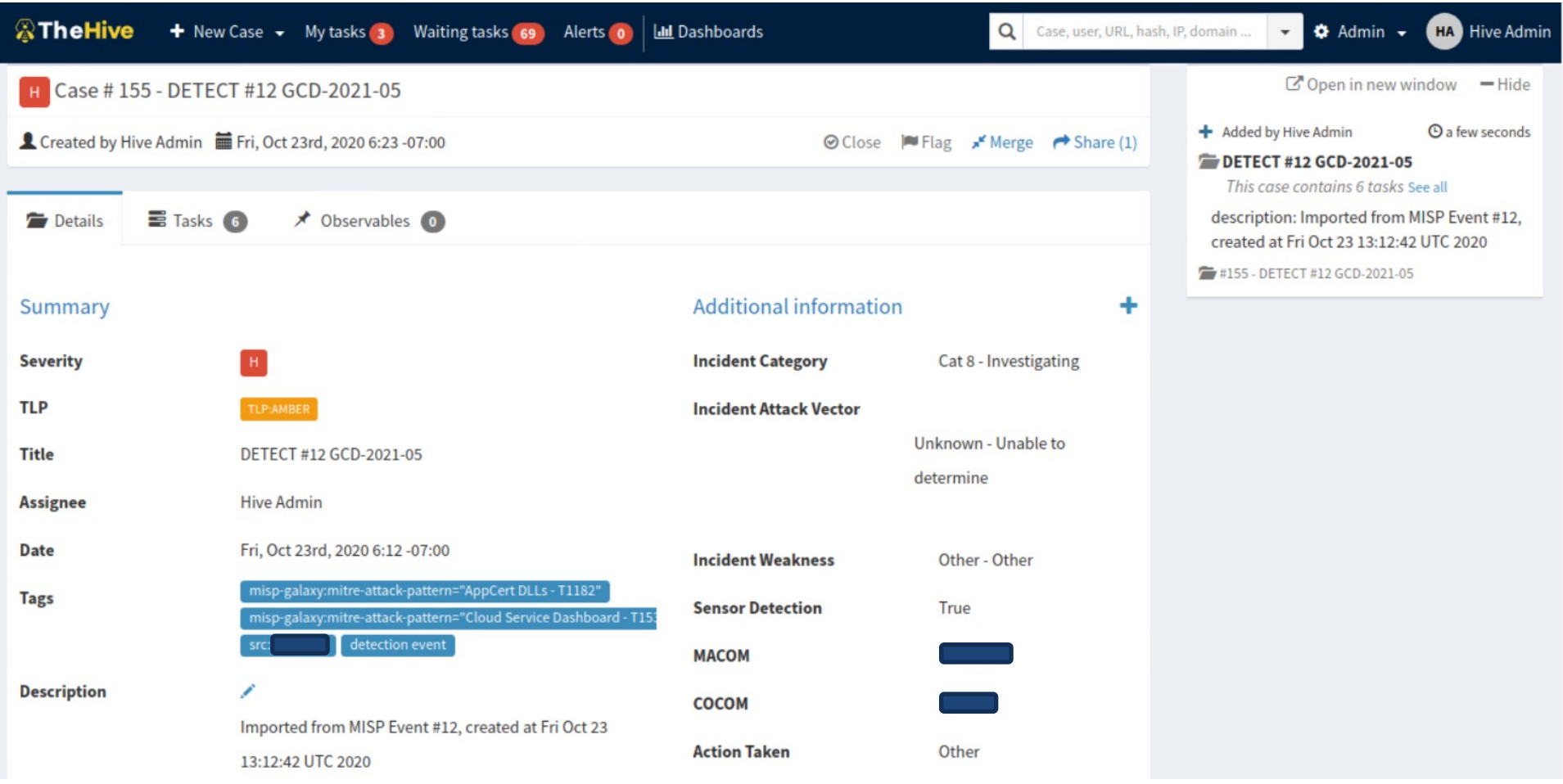



# What is Assessment?

# Assessment Challenges

How to identify:

- the highest performing teams?
- indicators/drivers of high performance?
- best practices from collected data?
- why some teams perform better?



# RCC-[redacted] - MC1 Deployment Timeline

| Time | Assigned | Event Description/Details | Execution Notes | Start | Complete | Status |
|---|---|---|---|---|---|---|
| +0:00 | [redacted] | Enable JWICS workstations on correct team | | (+0:00) | (+0:00) | |
| +0:00 | [redacted] | Comms Check<br>Start Zoom call<br>Comms check for chat groups / EO / HHQ / Nec Help Desk / Intel | | (+0:00) | (+0:00) | |
| +0:00 | [redacted] | Call STARTEX *20:06Z 14 OCT 2020* | | (+0:00) | (+0:00) | |
| +0:35 | [redacted] | CWD-2020-43 D'oh! - STEP 1<br>User browses to, downloads and installs Cobalt Strike Beacon<br>T1204 User Execution<br>Telemetry, User Behavior<br>Related Quiz Questions:<br>• Quiz 1: Question 4<br>• Quiz 1: Question 5<br>• Quiz 1: Question 6<br>Related EO Assessment:<br>• Conduct Defensive Cyberspace Operations:Conduct Cyberspace Operations (13-RCC-9000)<br>• Conduct Defensive Cyberspace Operations:Conduct Cyberspace Operations (13-RCC-9000) | +0:32 ADMIN [redacted]<br>Shifting Ops machine to 1.1 | (+0:34) | (+0:37) | |
| +0:35 | [redacted] | CWD-2020-43 D'oh! - STEP 2<br>Cobalt Strike Beacon connects to C2 via DNS over HTTPS<br>T1102 Command and Control - Web Service, T1071 Command and Control - Standard Application Layer Protocol<br>Telemetry Related Quiz Questions:<br>• Quiz 1: Question 4<br>• Quiz 1: Question 5<br>• Quiz 1: Question 6<br>Related EO Assessment:<br>• Conduct Defensive Cyberspace Operations:Conduct Cyberspace Operations (13-RCC-9000)<br>• Conduct Defensive Cyberspace Operations:Conduct Cyberspace Operations (13-RCC-9000) | +0:44 OBSRV [redacted]<br>Team had splunk mis-configured<br>+0:42 ADMIN [redacted]<br>Observed something related on the range | (+0:34) | (+0:37) | |
| +0:35 | [redacted] | CWD-2020-43 D'oh! - STEP 3<br>From C2, red operators execute ad-hoc commands on user workstation<br>T1041 Exfiltration - Exfiltration Over Command and Control Channel, T1048 Exfiltration - Exfiltration Over Alternative Protocol<br>Telemetry Related Quiz Questions:<br>• Quiz 1: Question 4<br>• Quiz 1: Question 5<br>• Quiz 1: Question 6<br>Related EO Assessment:<br>• Conduct Defensive Cyberspace Operations:Conduct Cyberspace Operations (13-RCC-9000)<br>• Conduct Defensive Cyberspace Operations:Conduct Cyberspace Operations (13-RCC-9000) | +0:38 IRESP Case #6 Created | (+0:34) | (+0:37) | |
| +0:40 | [redacted] | Quiz #1 In Process | | (+0:40) | (+0:40) | |
| +0:45 | [redacted] | CWD-2019-57 DNS Data Exfiltration<br>Data from NEC Users is exfiltrated using legitimate DNS queries | | (+0:42) | | |
| +1:25 | [redacted] | CWD-2020-43 Black Hole Memes<br>blackholememes.com installs a RAT on user machine | | | | |
| +0:55 | [redacted] | Quiz #2 Not Started | | | | |
| +3:15 | [redacted] | Call ENDEX | | | | |
| +3:15 | [redacted] | Turn off Cyclone traffic generation | | | | |

Add new timeline event

# What Value We Can Offer

# Value Proposition

Cyber Ranges

- DFARS Compliant
- PIV Authentication
- Open-Source Software
- Open Standards

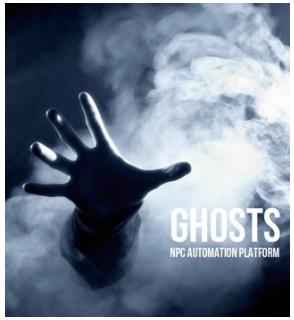
Expertise & Creativity

- Cyber Modeling and Simulation
- Threat Emulation
- Scenario Development
- Immersive Experiences
- Cybersecurity
- Threat Hunting

# To Learn More… Our Open-Source Software

## Crucible: A Cyber Simulation Application Framework

- Fact Sheet: https://resources.sei.cmu.edu/asset_files/FactSheet/2020_010_001_643855.pdf
- Code: https://github.com/cmu-sei/crucible
- Documentation: https://cmu-sei.github.io/crucible/
- Containers: https://hub.docker.com/u/cmusei




## GHOSTS Non-Player-Character Automation and Orchestration Framework

- Fact Sheet: https://resources.sei.cmu.edu/asset_files/FactSheet/2019_010_001_551085.pdf
- Code: https://github.com/cmu-sei/ghosts
- Documentation: https://github.com/cmu-sei/GHOSTS/wiki
- Containers: https://hub.docker.com/r/cmusei/ghosts

# To Learn More… Our Research Publications

## Technical Reports

- Dec 2021: Using Machine Learning to Increase NPC Fidelity
- May 2021: Foundation of Cyber Ranges
- Dec 2018: GHOSTS in the Machine: A Framework for Cyber-Warfare Exercise NPC Simulation
- Sep 2017: R-EACTR: A Framework for Designing Realistic Cyber Warfare Exercises

## Presentations

- Jun 2021: GHOSTS in the Machine: Orchestrating a Realistic Cybersecurity Exercise Battlefield

## Podcasts

- Oct 2022: ML-Driven Decision Making in Realistic Cyber Exercises

## Blogs

- Sep 2022: Using Alternate Data Streams in the Collection and Exfiltration of Data
- Apr 2022: Using Machine Learning to Increase the Fidelity of Non-Player Characters in Training Simulations
- Apr 2021: Generating Realistic Non-Player Characters for Training Cyberteams

# Contact Us


John Yarger
yarger@cert.org

Geoff Dobson
gdobson@cert.org

Tom Podnar
tgpodnar@cert.org

Dustin Updyke
ddupdyke@cert.org