Use Cases
Persistent Cyber Training Environment (PCTE)
Cyber Innovation Challenge #3
Attachment 2

06 July 2018

To provide context to the required capabilities, the following examples serve as use cases to better explain Technical Management Dashboard, White Cell (Exercise Control) and Assessments.

Technical Management Dashboard Use Case

This use case describes the escalating actions taken when a technical problem occurs during the execution of a training event and includes the training audience (Blue Team), White Cell (Exercise Control), Event Help Desk, Event Technical Support, PCTE Technical Operations Help Desk and associated Technical Operations Technicians. This use illustrates Technical Management Dashboard delivering the set of services, interactions, capabilities across PCTE users and product to enable the coordination, collaboration and execution of the platform, infrastructure and applications.

A. Blue Team Action

1. During a training event a Blue Team member runs into a technical issue with the environment he cannot resolve
2. The Blue Team member opens a trouble ticket via a trouble ticketing system available via the Technical Management Dashboard and a initiates a chat session with the White Cell and other relevant personnel to get a solution

B. White Cell (Exercise Control) Action

1. White cell determines the issue is not part of the training event and requires elevation
2. White contacts Event Help Desk to investigate

C. Event Help Desk Action

One of two options can occur depending on the Event Help Desk findings.

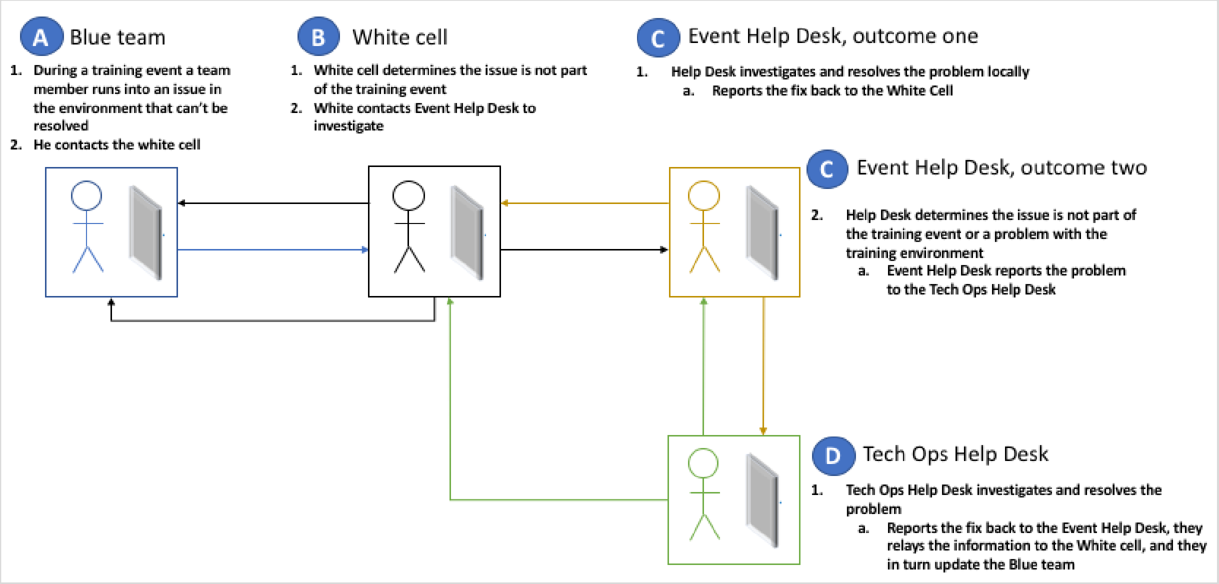
1. The Event Help Desk passes the request to technicians who use an event technical support application to interface with and troubleshoot the environment, to determine if they can resolve the problem locally.
    a. If so the Event Help Desk reports the fix back to the White Cell, and they in turn update the Blue Team

    Or

2. The Event Help Desk determines the issue is not part of the training event or the training environment
    a. The Event Help Desk reports the problem to the Technical Operations Help Desk

D. Technical Operations Help Desk Action

1. The Technical Operations Help Desk passes the ticket to technicians who use aspects of the Technical Management Dashboard to interface with and troubleshoot the underlying IT infrastructure/platform to resolve the issue
    a. The Technical Operations Help Desk reports the fix back to the Event Help Desk, they relay the information to the White Cell, and they in turn update the Blue Team



A Blue team

1. During a training event a team member runs into an issue in the environment that can't be resolved
2. He contacts the white cell

B White cell

1. White cell determines the issue is not part of the training event
2. White contacts Event Help Desk to investigate

C Event Help Desk, outcome one

1. Help Desk investigates and resolves the problem locally
    a. Reports the fix back to the White Cell

C Event Help Desk, outcome two

2. Help Desk determines the issue is not part of the training event or a problem with the training environment
    a. Event Help Desk reports the problem to the Tech Ops Help Desk

D Tech Ops Help Desk

1. Tech Ops Help Desk investigates and resolves the problem
    a. Reports the fix back to the Event Help Desk, they relays the information to the White cell, and they in turn update the Blue team

Assessment Use Case (Training and System Performance)

Technical Operations, Training Planners, and Training Managers use PCTE Assessment Tools to Gather System Performance and Utilization data as well as and Team Readiness Information.

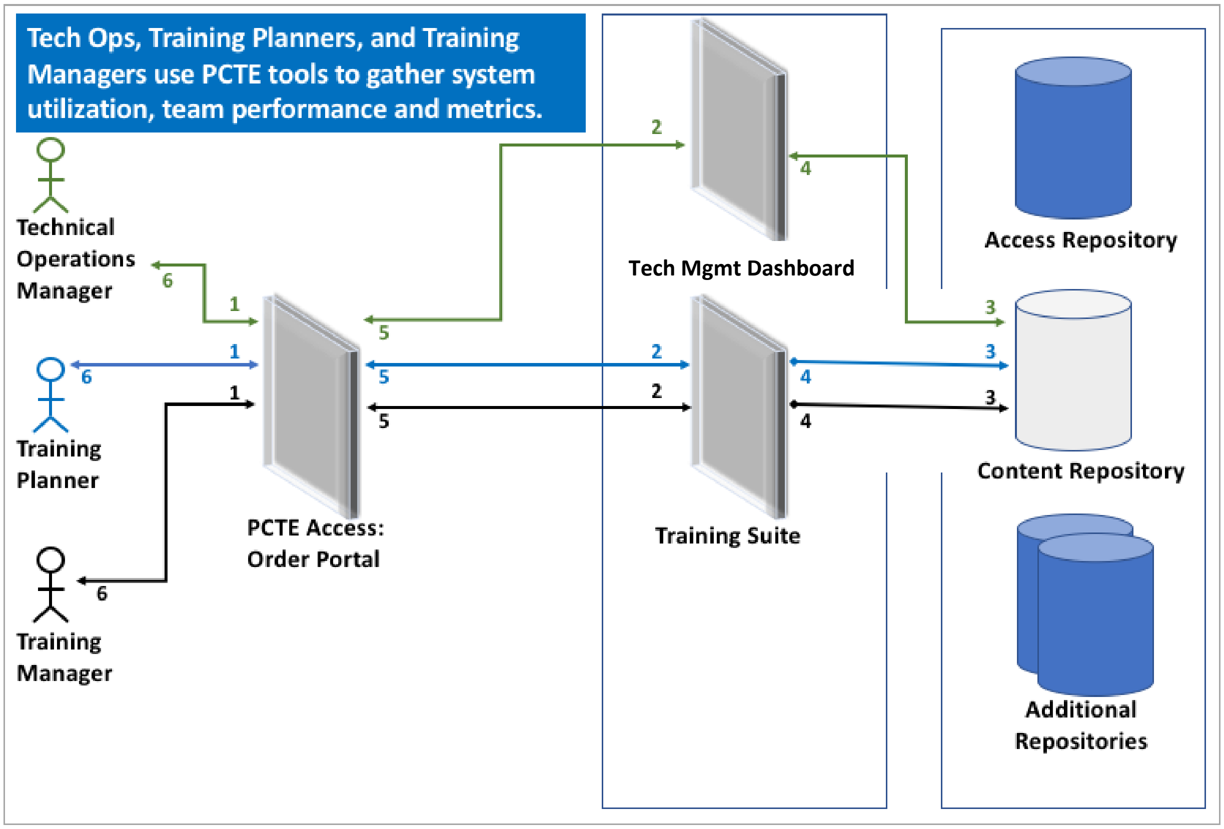
Users access PCTE for a variety of metrics. Technical Operators are considering the utilization, health and status of IT resources and are using the information to inform configuration or investment decisions with regard to the performance of the platform itself, supporting infrastructure and IT systems via the Technical Management Dashboard.

Team Leads/Training Planners are interested in the specific performance of their team on both individual and collective tasks. They will look at performance during events and over a period of several training sessions. Unit Training Managers may also use the system to see aggregated views over a period of time or throughout an exercise or training event. The following three scenarios describe typical metrics these types of users may require from PCTE.

1. A Technical Operator logs onto the system accessing the Technical Management Dashboard suite of tools and requests PCTE utilization metrics to include the load conditions for the past three cyber team level events on specified IT resources to inform and adjust forecast future resource allocation as required.

2. A Team Lead/Training Planner accesses the system. Using the role based authorities for a Team Lead/Training Planner, she requests training performance metrics for the individuals on her team as well as the team's performance as a whole based on their most recent training events.

3. A CNMF Training Manager accesses PCTE and requests statistics on all CNMF team events conducted over the last 6 months to include individual through force level training throughput as well as an aggregate view of performance metrics of his CNMF individual team members and his CNMF teams as a whole.



Tech Ops, Training Planners, and Training Managers use PCTE tools to gather system utilization, team performance and metrics.

Steps as shown in diagram	Description
1	Technical Operators accesses the PCTE through the Order Portal.

2, 3, 4, 5, 6	Technical Operator requests PCTE utilization metrics including load conditions for the past three cyber team level events on specified IT resources via the Technical Management Dashboard. Technical Operators uses the Technical Management Dashboard to gather the relevant data from the Content Repository.
1	Training Planner accesses the PCTE through the Order Portal.
2, 3, 4, 5, 6	Training Planner requests metrics on her individuals' and collective team's performance over the past 2 months. Training Planner uses the Training Suite to gather the relevant data from the Content Repository.
1	Training Manager accesses the PCTE through the Order Portal.
2, 3, 4, 5, 6	Training Manager requests statistics on all team events by the CNMF over the last 9 months to include team throughput and individual/collective performance metrics. Training Manager uses the Training Suite to gather the relevant data from the Content Repository.

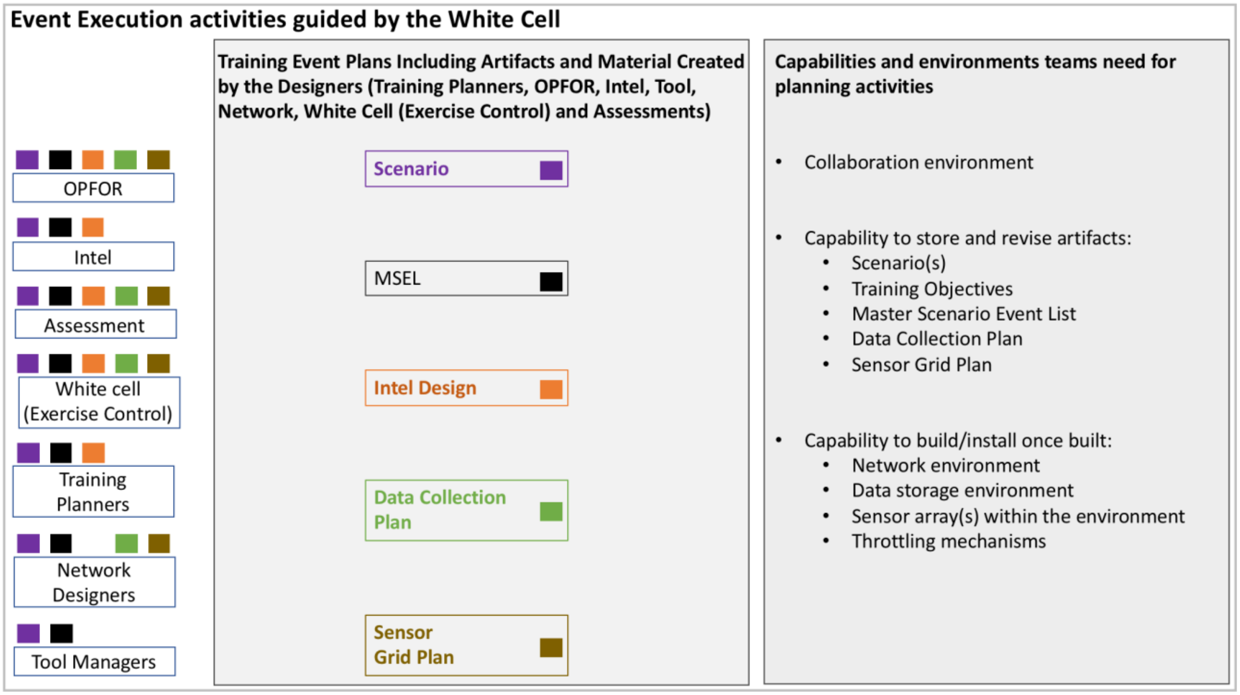
White Cell (Exercise Control) Planning Use Case

1. Training Planners want to train their teams on [x, y, z].
2. They review existing training objectives stored in PCTE and find several that could be modified for their needs.
3. They review existing scenarios stored in PCTE and find (one or several) that have most of the necessary pieces and could be used as a template or starting point for a new scenario.
4. Using the modified training objectives and scenario vignettes the Training Planners collaborate with Event Designers, including: White Cell, Blue Cell/Training Audience, OPFOR, Intel, Tool and Network Designers, to create more complete training material such as:
    - Training objectives
    - Scenarios with realistic training conditions
    - MSEL
    - Data Collection Plan for range resources as well as training audience performance assessments
    - Sensor Grid Plan for range resources as well as training audience performance assessments
5. Using these revised materials
    - OPFOR designs the red campaign plan and particular actions within the training scenario with appropriate injects and other offensive measures
    - Training Planners collaborate with Intel and Tool design team to develop appropriate Intel artifacts and injects as well as insert or connect appropriate tools and training materials into the scenario
    - Network Designers develop network schema/environment to accommodate the training objectives and scenarios and all requirements from the Blue Cell, White Cell, OPFOR, Network Designers and Tool Cell teams.

- Network Designers develop a plan for placement of sensors within the environment to accommodate Technical Operations and White Cell assessment plans
- Network Designers develop a plan for storage of assessment data
- White Cell, Network Designers, and OPFOR determine ways to throttle (slow down or speed up) the pace/rhythm/tempo of the training in order to allow the training audience to meet their objectives.

6. White Cell oversees and coordinates all of these efforts including testing of:
   - Environment(s) to ensure they meet training objectives
   - Sensors and throttling mechanisms to meet assessment (training audience and event resource performance) criteria
   - Artifacts to ensure they are accurate and supporting the MSEL

The diagram below shows the Event Management design elements on the left, the types of planning materials that are created in the middle and the capabilities required to accommodate the planning activities on the right. The colored squares are intended to show which groups have input to which training materials.


Event Execution activities guided by the White Cell
Training Event Plans Including Artifacts and Material Created by the Designers (Training Planners, OPFOR, Intel, Tool, Network, White Cell (Exercise Control) and Assessments)
Capabilities and environments teams need for planning activities
🟪 ⬛ 🟧 🟩 🟫
OPFOR
🟪 ⬛ 🟧
Intel
🟪 ⬛ 🟧 🟩 🟫
Assessment
🟪 ⬛ 🟧 🟩 🟫
White cell (Exercise Control)
🟪 ⬛ 🟧
Training Planners
🟪 ⬛ 🟩 🟫
Network Designers
🟪 ⬛
Tool Managers
Scenario 🟪
MSEL ⬛
Intel Design 🟧
Data Collection Plan 🟩
Sensor Grid Plan 🟫
• Collaboration environment
• Capability to store and revise artifacts:
• Scenario(s)
• Training Objectives
• Master Scenario Event List
• Data Collection Plan
• Sensor Grid Plan
• Capability to build/install once built:
• Network environment
• Data storage environment
• Sensor array(s) within the environment
• Throttling mechanisms

<u>White Cell (Exercise Control) Event Execution Activities Use Case</u>

In the use case below a multi-team training exercise is in progress. This example represents one of many types of training events available from the PCTE. Thus, PCTE must be able to scale from a single team member training on a particular skill, or circumstance to a Force Level Training Events (multiple teams with different headquarters elements directing them) and Mission Rehearsal Training Events.

The White Cell is monitoring a multi-team exercise. Three Blue Cyber Protection Teams from three different services (Air Force, Army and Navy) with Intel support are conducting a Defensive Cyberspace Operations (DCO) training event.

One Blue Team has identified and is in the process of removing all the threats/exploits posed by OPFOR. The second Blue Team has identified a few of OPFOR's exploits and is working on removing them from their portion of the network, while continuing to search for other intrusions. The third Blue Team is conducting a hunt mission but is struggling to identify any of the OPFOR's actions or artifacts. OPFOR is operating in this Blue Team's area of operations and is in the process of extracting critical/classified information from the Blue network.

The White Cell is monitoring the performance of all three Blue Teams as well as that of OPFOR through network monitoring tools capturing actions taken in the scenario and through observer / controller personnel embedded with the Blue Teams. The observer / controller communicates with the White Cell through automated reports, chat mechanisms and during hot washes and after action reviews. The White Cell recognizes they need to intervene to stop slow the work of OPFOR in the third Blue Team's area. The White Cell modifies the MSEL injects to throttle the pace of the training for this third team and slows the OPFOR's actions as well.

The White Cell also has visualization(s) of network performance and receives alerts when critical network performance indicators are beyond thresholds. The also receive reports and alerts from the observer / controller teams to indicate actions to take. These network visualizations and observer / controller alerts some of the many way(s) the White Cell monitors the various network sensors to ensure:

- The network is performing optimally
- The assessors have a clear picture of how the various teams are performing
- Appropriate metrics are collected for later analysis and assessment
- Effective playback for hot washes and team evaluation/learning

<u>White Cell Event Post-Execution Activities Use Case</u>

In the use case below a multi-team training exercise is in progress. This example represents one of many types of training events available from the PCTE. Thus, PCTE must be able to scale from a single team member training on a particular skill, or circumstance to a Force Level Training Events (multiple teams with different headquarters elements directing them) and Mission Rehearsal Training Events.

The White Cell (Exercise Control) is monitoring a multi-team exercise. Three Blue Cyber Protection Teams from three different services (Air Force, Army and Navy) with Intel support are conducting a Defensive Cyberspace Operations (DCO) training event.

One Blue Team has identified and is in the process of removing all the threats/exploits posed by OPFOR. The second Blue Team has identified a few of OPFOR's exploits and is working on removing them from their portion of the network, while continuing to search for other intrusions. The third Blue Team is conducting a hunt mission but is struggling to identify any of the OPFOR's actions or artifacts. OPFOR is operating in this Blue Team's area of operations and is in the process of extracting critical/classified information from the Blue network.

The White Cell (Exercise Control) is monitoring the performance of all three Blue Teams as well as that of OPFOR through network monitoring tools capturing actions taken in the scenario and through observer / controller personnel embedded with the Blue Teams. The observer / controller communicates with the White Cell (Exercise Control) through automated reports, chat mechanisms and during hot washes and after action reviews. The White Cell (Exercise Control) recognizes they need to intervene to stop slow the work of OPFOR in the third Blue Team's area. The White Cell (Exercise Control) modifies the MSEL injects to throttle the pace of the training for this third team and slows the OPFOR's actions as well.

The White Cell (Exercise Control) also has visualization(s) of network performance and receives alerts when critical network performance indicators are beyond thresholds. The also receive reports and alerts from the observer / controller teams to indicate actions to take. These network visualizations and observer / controller alerts some of the many way(s) the White Cell (Exercise Control) monitors the various network sensors to ensure:

- The network is performing optimally
- The assessors have a clear picture of how the various teams are performing
- Appropriate metrics are collected for later analysis and assessment
- Effective playback for hot washes and team evaluation/learning

White Cell (Exercise Control) Event Post-Execution Activities Use Case

During a Force level exercise with multiple CMF teams and multiple headquarters elements (i.e. Joint Force Headquarters – Cyber and Joint Force Headquarters DoD Information Networks), data has been collected via automated sensors and individual observations from the participants and White Cell (Exercise Control) observers each day. This includes the data assessment sensors placed throughout the environment such as automated actions of Blue Teams and OPFOR as well as electronically entered feedback from the Blue Teams, Observer Controllers and the OPFOR. It also includes the technical feedback from the Event Support Cell on the performance of the range and associated resources supporting the event. The White Cell (Exercise Control) analyzes the collected data in order to:

1. Assess the performance of the training audience
2. Assess the performance of various aspects of the hardware/software in the environment
3. Improve content, designs, communication, planning and other elements for future training exercises.

To evaluate team performance, the assessment team members use data recorded in PCTE including assessor observations, sensor data and playback capabilities. Planners and assessors then meet with each training audience element separately to review the performance data. Subsequently, scores for the performance of each training audience element, including individuals' performance are recorded into content repositories accessible by training managers. These scores are stored in as flight log data would be for pilots. The individual and team performance data (flight log data) is stored in association with the situation/circumstances under which they were collected, for example, the type of network, types of nodes complexity of the network enclaves, information about the nature and timeliness of the Intel provided, and the nature of the OPFOR injects.

To assess the performance of the hardware/software used in the environment appropriate members of the White Cell, meet with their counterparts from Network Designers, Tool Managers and Event Support Cell to evaluate the effectiveness of the environment in meeting the training objectives. The reliability and availability are also assessed and recorded for various stakeholders' visibility.

Finally, appropriate members of both groups described above will meet to decide what from the current exercise should be stored in the PCTE Content Repository for example, network design, tool design, and playback documents. Additionally, they analyze the performance of the environment and its ability to support the training as well as the performance of the other participants including the OPFOR, the Intelligence support, the Tool Managers and the Event Support Cell. They also consider the developed products and their effectiveness in meeting the needs of the training audience. The culmination of this analysis is summarized in the after-action review of the event for the Event Directors, Training Managers, USCYBERCOM J7 and other key stakeholders of the event. The White Cell (Exercise Control) leads the after-action review and executes an automated replay of events as required to highlight the analysis.